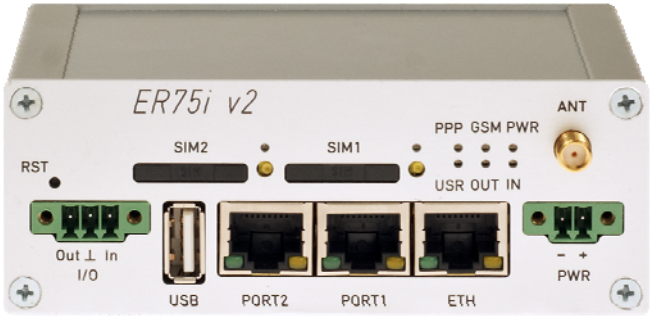
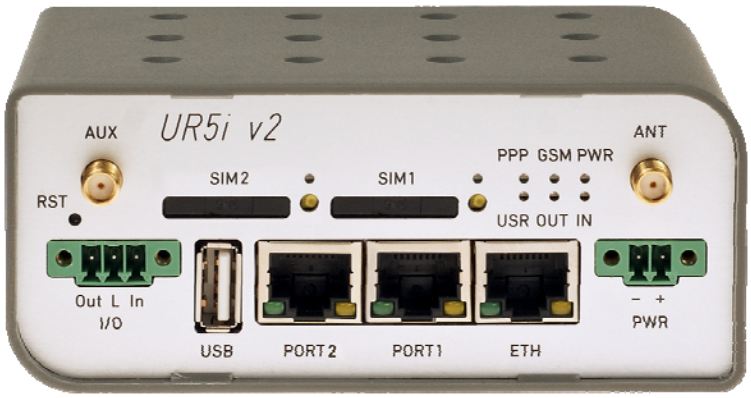
WWW.INFOPULSAS.LT
info@infopulsas.lt

CONFIGURATION MANUAL

for v2 routers





Used symbols

Danger – important notice, which may have an influence on the user's safety or the function of the device.

Attention – notice on possible problems, which can arise in specific cases.

Information, notice – information, which contains useful advice or special interest.

Firmware version

Actual version of firmware is 3.0.1 (26.9.2011).

GPL license

Source codes under GPL license are available free of charge by sending an email to info@conel.cz.

Routers version

Properties and settings of router associated with the GSM connection is not available in industrial router XR5i v2.

PPPoE configuration item is only available on the industrial router XR5i v2, used to set the PPPoE connection over Ethernet.

Declared quality system
ISO 9001

Contents

1. Configuration settings over web browser 1
   1.1. Secured access to web configuration 2
   1.2. Network status 3
   1.3. DHCP status 4
   1.4. GPRS/UMTS status 5
   1.5. IPsec status 7
   1.6. DynDNS status 7
   1.7. System log 8
   1.8. LAN configuration 9
   1.9. VRRP configuration 13
   1.10. GPRS configuration 15
      1.10.1. GPRS connection 15
      1.10.2. DNS address configuration 16
      1.10.3. Check PPP connection configuration 16
      1.10.4. Data limit configuration 16
      1.10.5. Switch between SIM cards configuration 17
      1.10.6. Dial-In access configuration 18
      1.10.7. PPPoE bridge mode configuration 18
   1.11. PPPoE configuration 21
   1.12. Firewall configuration 22
   1.13. NAT configuration 24
   1.14. OpenVPN tunnel configuration 27
   1.15. IPSec tunnel configuration 31
   1.16. GRE tunnels configuration 35
   1.17. L2TP tunnel configuration 37
   1.18. DynDNS client configuration 39
   1.19. NTP client configuration 40
   1.20. SNMP configuration 41
   1.21. SMTP configuration 44
   1.22. SMS configuration 45
      1.22.1. Send SMS 46
   1.23. Expansion port configuration 52
   1.24. USB port configuration 55
   1.25. Startup script 58
   1.26. Up/Down script 59
   1.27. Automatic update configuration 60
   1.28. User modules 61
   1.29. Change profile 62
   1.30. Change password 62
   1.31. Set real time clock 63
   1.32. Set SMS service center address 63
   1.33. Unlock SIM card 63
   1.34. Send SMS 64
   1.35. Backup configuration 64
   1.36. Restore configuration 64
   1.37. Update firmware 65
   1.38. Reboot 65
2. Configuration setting over Telnet 66

Picture list

Fig. 1: Web configuration 1
Fig. 2: Network status 4
Fig. 3: DHCP status 4
Fig. 4: GPRS status 6
Fig. 5: IPsec status 7
Fig. 6: DynDNS status 7
Fig. 7: System log 8
Fig. 8: Example program syslogd start with the parameter -r 8
Fig. 9: Topology of example LAN configuration 1 10
Fig. 10: Example LAN configuration 1 10
Fig. 11: Topology of example LAN configuration 2 11
Fig. 12: Example LAN configuration 2 11
Fig. 13: Topology of example LAN configuration 3 12
Fig. 14: Example LAN configuration 3 12
Fig. 15: Topology of example VRRP configuration 14
Fig. 16: Example VRRP configuration – main router 14
Fig. 17: Example VRRP configuration – backup router 14
Fig. 18: GPRS configuration 19
Fig. 19: Example of GPRS configuration 1 20
Fig. 20: Example of GPRS configuration 2 20
Fig. 21: Example of GPRS configuration 3 20
Fig. 22: PPPoE configuration 21
Fig. 23: Topology of example firewall configuration 23
Fig. 24: Example firewall configuration 23
Fig. 25: Topology of example NAT configuration 25
Fig. 26: Example NAT configuration 1 25
Fig. 27: Topology of example NAT configuration 26
Fig. 28: Example of NAT configuration 2 26
Fig. 29: OpenVPN tunnels configuration 27
Fig. 30: OpenVPN tunnel configuration 29
Fig. 31: Topology of example OpenVPN configuration 30
Fig. 32: IPsec tunnels configuration 31
Fig. 33: IPsec tunnel configuration 33
Fig. 34: Topology of example IPsec configuration 34
Fig. 35: GRE tunnels configuration 35
Fig. 36: GRE tunnel configuration 36
Fig. 37: Topology of GRE tunnel configuration 36
Fig. 38: L2TP tunnel configuration 37
Fig. 39: Topology of example L2TP tunnel configuration 38
Fig. 40: Example of DynDNS configuration 39
Fig. 41: Example of NTP configuration 40
Fig. 42: Example of SNMP configuration 43
Fig. 43: Example of the MIB browser 43
Fig. 44: SMTP client configuration 44
Fig. 45: SMTP configuration 44
Fig. 46: Example of SMS configuration 1 48
Fig. 47: Example of SMS configuration 2 49
Fig. 48: Example of SMS configuration 3 50
Fig. 49: Example of SMS configuration 4 51

Fig. 50: Expansion port configuration 53
Fig. 51: Example of expansion port configuration 1 54
Fig. 52: Example of expansion port configuration 2 54
Fig. 53: USB configuration 56
Fig. 54: Example of USB port configuration 1 57
Fig. 55: Example of USB port configuration 2 57
Fig. 56: Startup script 58
Fig. 57: Example of Startup script 58
Fig. 58: Up/Down script 59
Fig. 59: Example of Up/Down script 59
Fig. 60: Example of automatic update 1 61
Fig. 61: Example of automatic update 2 61
Fig. 62: User modules 61
Fig. 63: Change profile 62
Fig. 64: Change password 62
Fig. 65: Set real time clock 63
Fig. 66: Set SMS service center address 63
Fig. 67: Unlock SIM card 63
Fig. 68: Send SMS 64
Fig. 69: Restore configuration 64
Fig. 70: Update firmware 65
Fig. 71: Reboot 65

Table list

Table 1: Description of interface in network status 3
Table 2: Description of information in network status 3
Table 3: DHCP status description 4
Table 4: Description of GSM information item 5
Table 5: Description of period 5
Table 6: Description of GSM statistic 5
Table 7: Description of GSM traffic 5
Table 8: Possibly DynDNS report 7
Table 9: Configuration of network interface 9
Table 10: Configuration of dynamic DHCP server 9
Table 11: Configuration of static DHCP server 9
Table 12: VRRP configuration 13
Table 13: Check PPP connection 13
Table 14: GPRS connection configuration 15
Table 15: Check PPP connection configuration 16
Table 16: Data limit configuration 16
Table 17: Default and backup SIM configuration 17
Table 18: Switch between SIM card configurations 17
Table 19: Switch between SIM card configurations 18
Table 20: Dial-In access configuration 18
Table 21: PPPoE configuration 21
Table 22: Firewall configuration 22
Table 23: NAT configuration 24
Table 24: Configuration of send all incoming packets 24
Table 25: Remote access configuration 25
Table 26: Overview OpenVPN tunnels 27
Table 27: OpenVPN configuration 29
Table 28: Example OpenVPN configuration 30
Table 29: Overview IPsec tunnels 31
Table 30: IPsec tunnel configuration 32
Table 31: Example IPsec configuration 34
Table 32: Overview GRE tunnels 35
Table 33: GRE tunnel configuration 35
Table 34: Example GRE tunnel configuration 36
Table 35: L2TP tunnel configuration 37
Table 36: Example L2TP tunel configuration 38
Table 37: DynDNS configuration 39
Table 38: NTP configuration 40
Table 39: SNMP configuration 41
Table 40: SNMP configuration 41
Table 41: Object identifier for binary input and output 42
Table 42: Object identifier for CNT port 42
Table 43: Object identifier for M-BUS port 42
Table 44: Send SMS configuration 45
Table 45: Control via SMS configuration 45
Table 46: Control SMS 46
Table 47: Send SMS on serial PORT1 configuration 46
Table 48: Send SMS on serial PORT1 configuration 46
Table 49: Send SMS on ethernet PORT1 configuration 46

Table 50: AT commands for work with SMS 46
Table 51: Expansion PORT configuration 1 52
Table 52: Expansion PORT configuration 2 52
Table 53: CD signal description 52
Table 54: DTR signal description 53
Table 55: USB port configuration 1 55
Table 56: USB PORT configuration 2 55
Table 57: CD signal description 55
Table 58: DTR signal description 56
Table 59: Automatic update configuration 60
Table 60: Telnet commands 66

1. Configuration settings over web browser

Attention! If the SIM card is not inserted in the router, then wireless transmissions will not work. The inserted SIM card must have activated GPRS. Insert the SIM card when the router is switched-off.

Monitoring of the status, configuration and administration of the router can be performed by means of the web interface, which is available after insertion of IP address of the modem into the web browser. The default IP address of the modem is 192.168.1.1. Configuration may be performed only by the user "root" with initial password "root".

The left part of the web interface contains the menu with pages for monitoring of the Status, Configuration and Administration of the router.

Name of the router is displayed depending on type of your router. Items' Name and Location displays the name and location of the router filled in the SNMP configuration. (See SNMP Configuration).

For enhanced security of network managed router is must change the default password router. If the router's default password is set, the item "Change password" is highlighted in red.

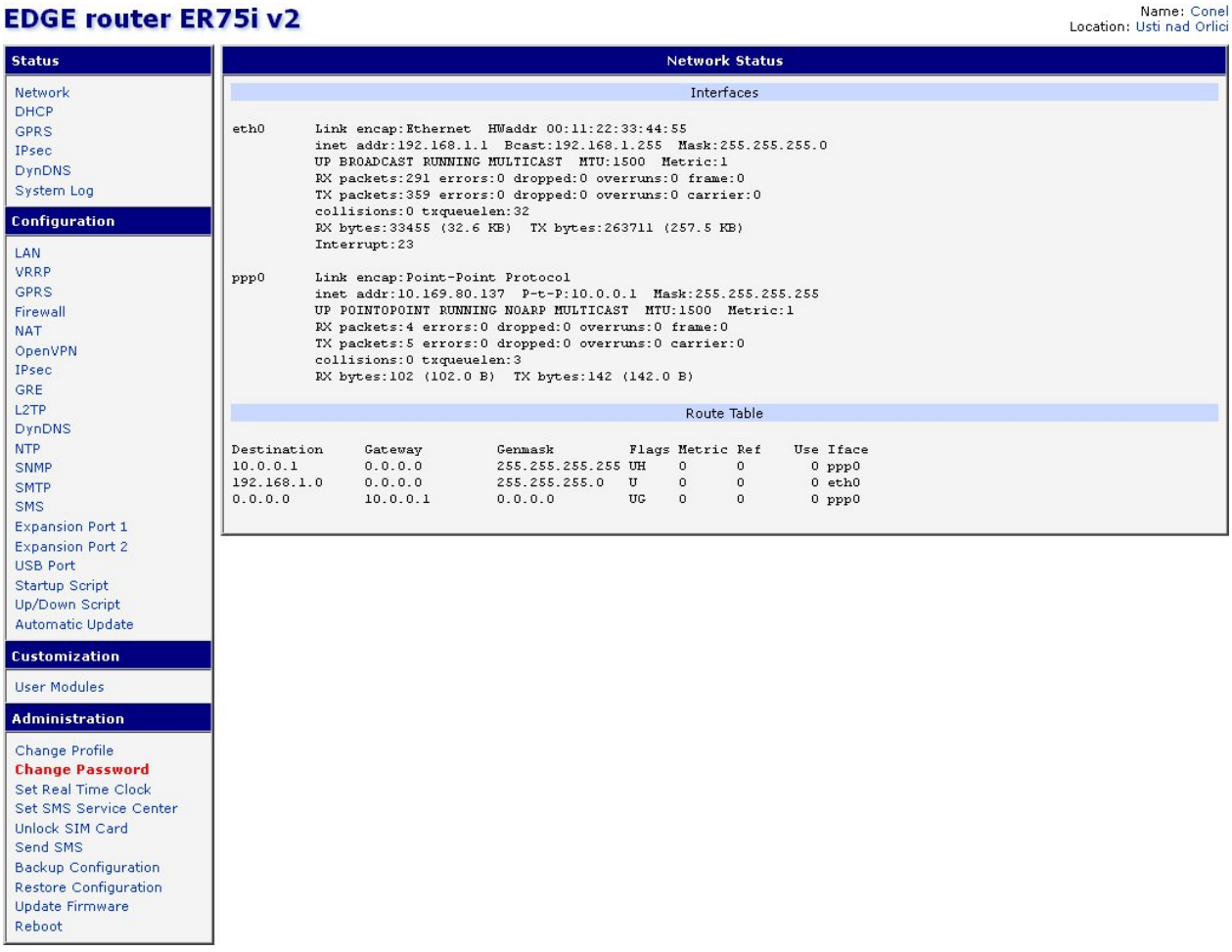


Fig. 1: Web configuration

After green LED starts to blink it is possible to restore initial settings of the router by pressing button RST on front panel. If press button RST, configuration is restored to default and it is reboot (green LED will be on).

1.1. *Secured access to web configuration*

To the web configuration can be accessed via a secure HTTPS protocol.

In the event of a default router IP address is a secure router configuration accessed by typing address https://192.168.1.1 in the web browser. The first approach is the need to install a security certificate. If your browser reports a disagreement in the domain, this message can be prevented use the following procedure.

Since the domain name in the certificate is given the MAC address of the router (such separators are used dashes instead of colons), it is necessary to access the router under this domain name. For access to the router via a domain name, it is adding a DNS record in the DNS table, the operating system.

- Editing /etc/hosts (Linux/Unix)
- Editing C:\WINDOWS\system32\drivers\etc\hosts (Windows XP)
- Configuring your own DNS server

In addition to configuring the router with MAC address 00:11:22:33:44:55 is accessed to secure configuration by typing address https://00-11-22-33-44-55 in the web browser. The first approach is the need to install a security certificate.

When using self signing certificate must upload your files and http_cert http_key directory /etc/certs in the router.

1.2. *Network status*

To view the system information about the router operation, select the ***Network*** menu item. The upper part of the window displays detailed information about active interfaces:

Interface	Description
eth0	Networks interface
ppp0	Interface (active connection to GPRS/EDGE)
tun0	OpenVPN tunnel interface
ipsec0	IPSec tunnel interface
gre1	GRE tunnel interface

Table 1: Description of interface in network status

By each of the interfaces is then shown the following information:

Item	Description
HWaddr	Hardware (unique) address of networks interface
inet	IP address of interface
P-t-P	IP address second ends connection
Bcast	Broadcast address
Mask	Mask of network
MTU	Maximum size of packet, which is equipment able transmit
Metric	Number of routers, over which packet must go trought
RX	• packets – received packets • errors - number of errors • dropped - dropped packets • overruns – incoming packets lost because of overload • frame – wrong incoming packets because of incorrect packet size
TX	• packets – transmit packets • errors - number of errors • dropped - dropped packets • overruns – outgoing packets lost because of overload • carrier - wrong outgoing packets with errors resulting from the physical layer
collisions	Number of collisions on physical layer
txqueuelen	Length of front network device
RX bytes	Total number of received bytes
TX bytes	Total number of transmitted bytes

Table 2: Description of information in network status

It is possible to read status PPP connection from the network information. If the PPP connection is active, then it is in the system information shown as ppp0 interface.

For industrial router XR5i v2, interface ppp0 indicates PPPoE connection.

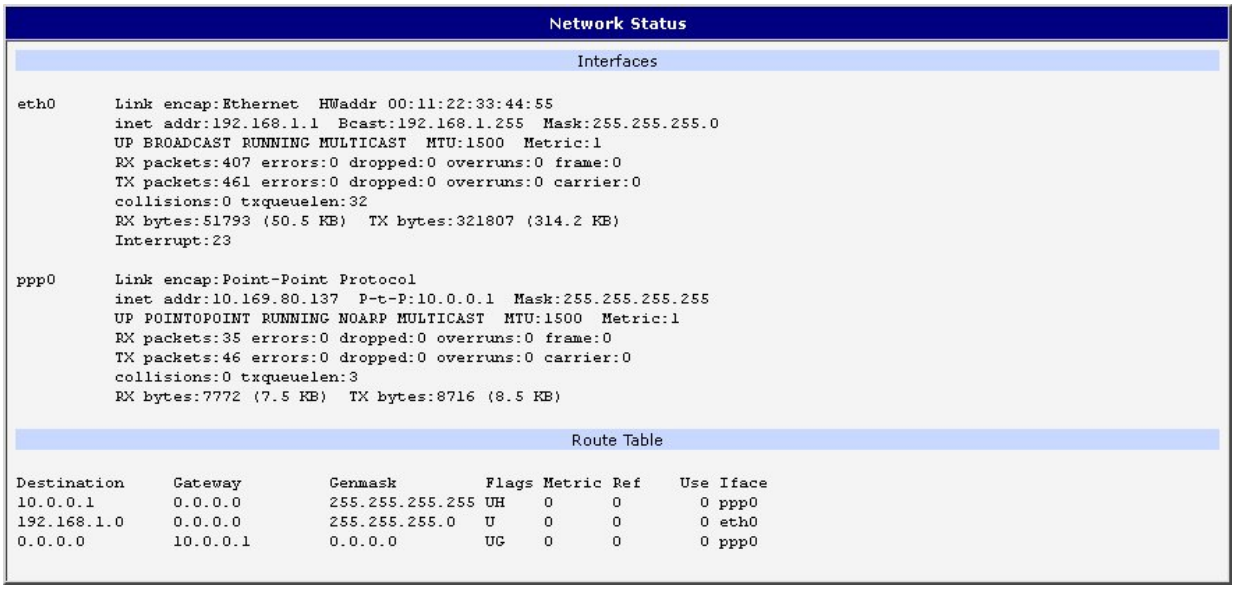


Fig. 2: Network status

1.3. *DHCP status*

Information on the activities of the DHCP server can be accessed by selecting the **DHCP status**.

DHCP status informs about activities DHCP server. The DHCP server provides automatic configuration of devices connected to the network managed router. DHCP server assigns to each device's IP address, netmask, default gateway (IP address of router) and DNS server (IP address of router).

For each configuration, the DHCP status window displays the following information.

Item	Description
lease	Assigned IP address
starts	Time of assignation of IP address
ends	Time of termination IP address validity
hardware ethernet	Hardware MAC (unique) address
uid	Unique ID
client-hostname	Computer name

Table 3: DHCP status description

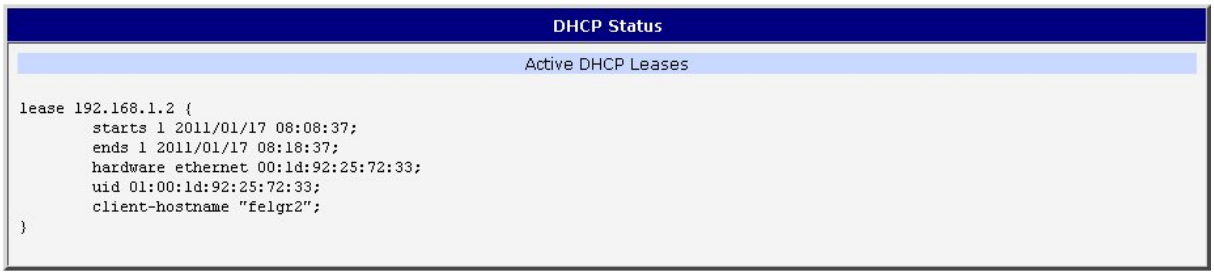


Fig. 3: DHCP status

In the extreme, the DHCP status can display two records for one IP address. That could have been caused by resetting of network cards.

1.4. *GPRS/UMTS status*

The industrial router XR5i v2 is not availability item **GPRS/UMTS status**.

GPRS menu item contains actual information about GPRS/UMTS connections.

Item	Description
PLMN	Code of operator
Cell	The cell to which the router is connected
Channel	The channel on which the router communicates
Level	The signal quality of the selected cell
Neighbours	Signal quality of neighboring hearing cells
Uptime	Time to establish PPP connection

Table 4: Description of GSM information item

If the neighbor cell is highlighted in red, risk of often switching between neighbor and actual cells.

The next section of this window displays information about the quality of the GPRS/UMTS connection in each period.

Period	Definition of the period
Today	Today from 0:00 to 23:59
Yesterday	Yesterday from 0:00 to 23:59
This week	This week from Monday 0:00 to Sunday 23:59
Last week	Last week from Monday 0:00 to Sunday 23:59
This period	This accounting period. The interval must be set in the GPRS Configuration
Last period	Last accounting period. The interval must be set in the GPRS Configuration

Table 5: Description of period

Item	Description
Level Min.	Minimal signal strength
Level Avg.	Average signal strength
Level Max.	Maximal signal strength
Cells	Number of switch between cells
Availability	Availability of PPP connection

Table 6: Description of GSM statistic

Availability is information in percentage, that is calculated us ration of PPP connect time and router power on time.

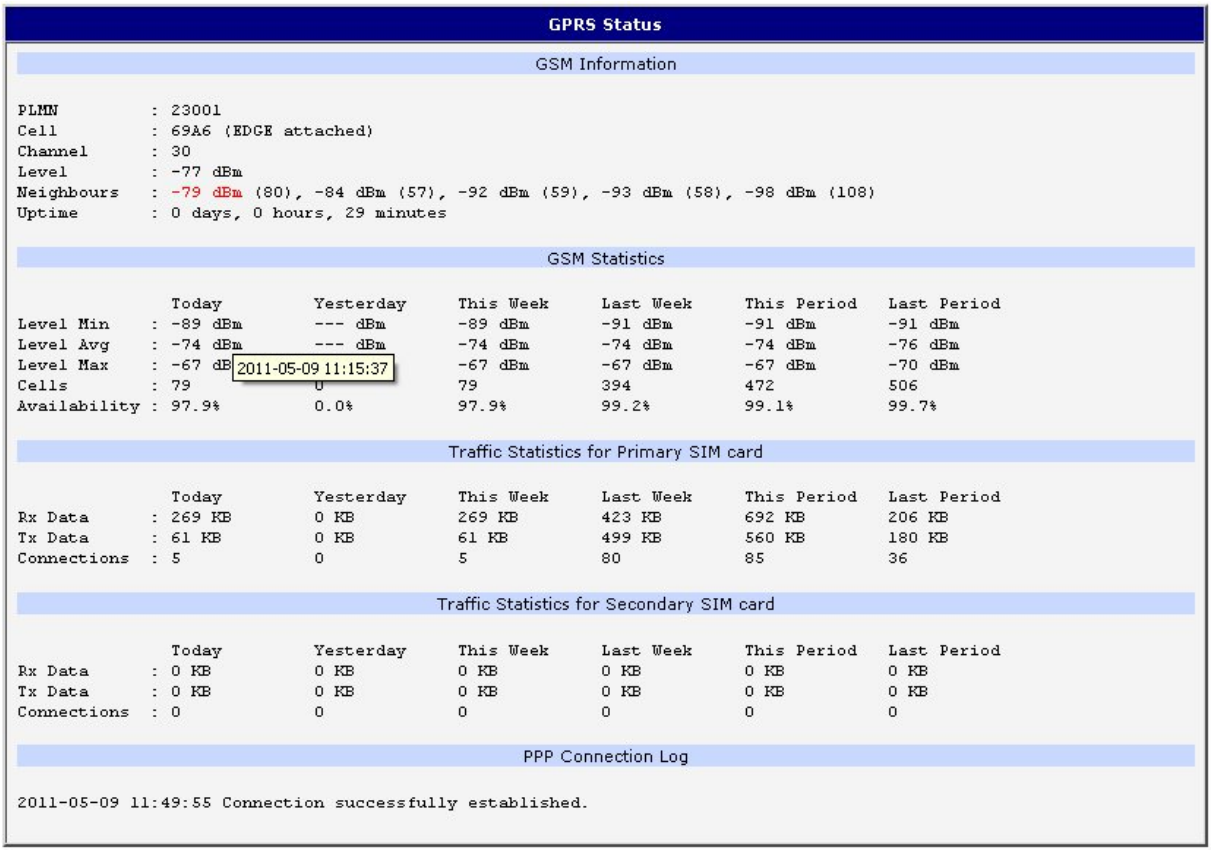
After you place your cursor on the maximum or minimum signal strength, will show the last time when the signal strength reaching the router.

In the middle part of window is shows information about transferred data and number of connection both SIM card, for each period

Item	Description
RX data	Total volume of received data
TX data	The total volume of data sent
Connections	Number of PPP connection establishment

Table 7: Description of GSM traffic

The PPP Connection Log is in the bottom of window, where are information about the make-up of the PPP connection and problems in establishment.



GPRS Status

GSM Information

```
PLMN          : 23001
Cell          : 69A6 (EDGE attached)
Channel       : 30
Level         : -77 dBm
Neighbours    : -79 dBm (80), -84 dBm (57), -92 dBm (59), -93 dBm (58), -98 dBm (108)
Uptime        : 0 days, 0 hours, 29 minutes
```

GSM Statistics

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Level Min	-89 dBm	--- dBm	-89 dBm	-91 dBm	-91 dBm	-91 dBm
Level Avg	-74 dBm	--- dBm	-74 dBm	-74 dBm	-74 dBm	-76 dBm
Level Max	-67 dB	2011-05-09 11:15:37	-67 dBm	-67 dBm	-67 dBm	-70 dBm
Cells	79	0	79	394	472	506
Availability	97.9%	0.0%	97.9%	99.2%	99.1%	99.7%

Traffic Statistics for Primary SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	269 KB	0 KB	269 KB	423 KB	692 KB	206 KB
Tx Data	61 KB	0 KB	61 KB	499 KB	560 KB	180 KB
Connections	5	0	5	80	85	36

Traffic Statistics for Secondary SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Tx Data	0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Connections	0	0	0	0	0	0

PPP Connection Log

```
2011-05-09 11:49:55 Connection successfully established.
```

Fig. 4: GPRS status

1.5. *IPsec status*

Information on actual IPsec tunnel state can be called up in option ***IPsec*** in the menu.

After correct build the IPsec tunnel, status display ***IPsec SA established*** (highlighted in red) in IPsec status information. Other information is only internal character.

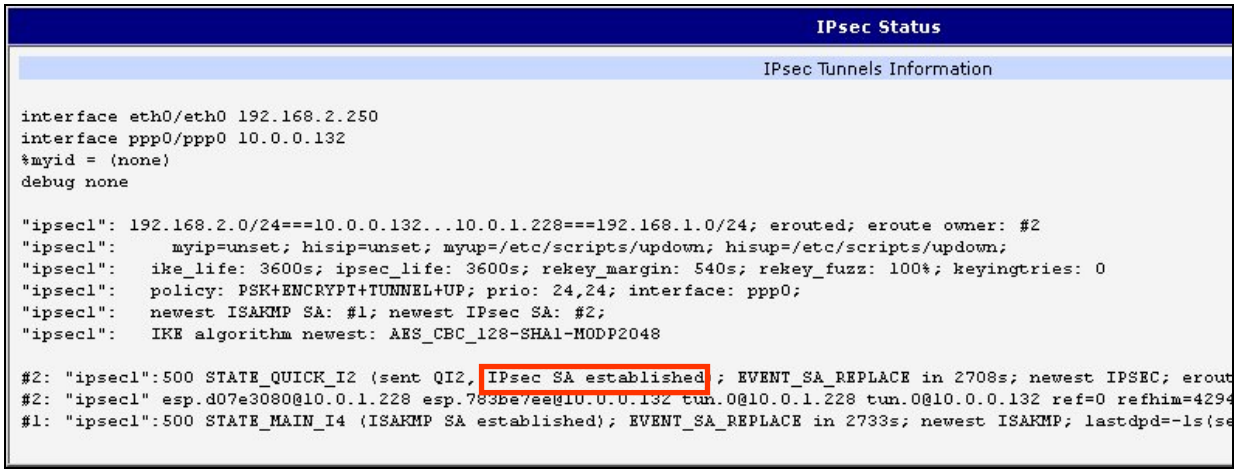


Fig. 5: IPsec status

1.6. *DynDNS status*

DynDNS up - dating entry result on server www.dyndns.org can be called up in option **DynDNS** item in the menu.

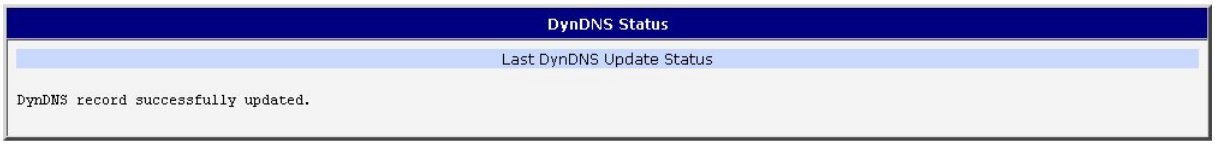


Fig. 6: DynDNS status

In detecting the status of updates DynDNS record are possible following message:

Report
DynDNS client is disabled.
Invalid username or password.
Specified hostname doesn't exist.
Invalid hostname format.
Hostname exists, but not under specified username.
No update performed yet.
DynDNS record is already up to date.
DynDNS record successfully update.
DNS error encountered.
DynDNS server failure.

Table 8: Possibly DynDNS report

For correct function DynDNS, SIM card of router must have assigned public IP address.

1.7. *System log*

In case of any problems with connection to GPRS it is possible to view the system log by pressing the ***System Log*** menu item. In the window, are displayed detailed reports from individual applications running in the router. By the help of button *Save* it is possible to save the system log to the computer.

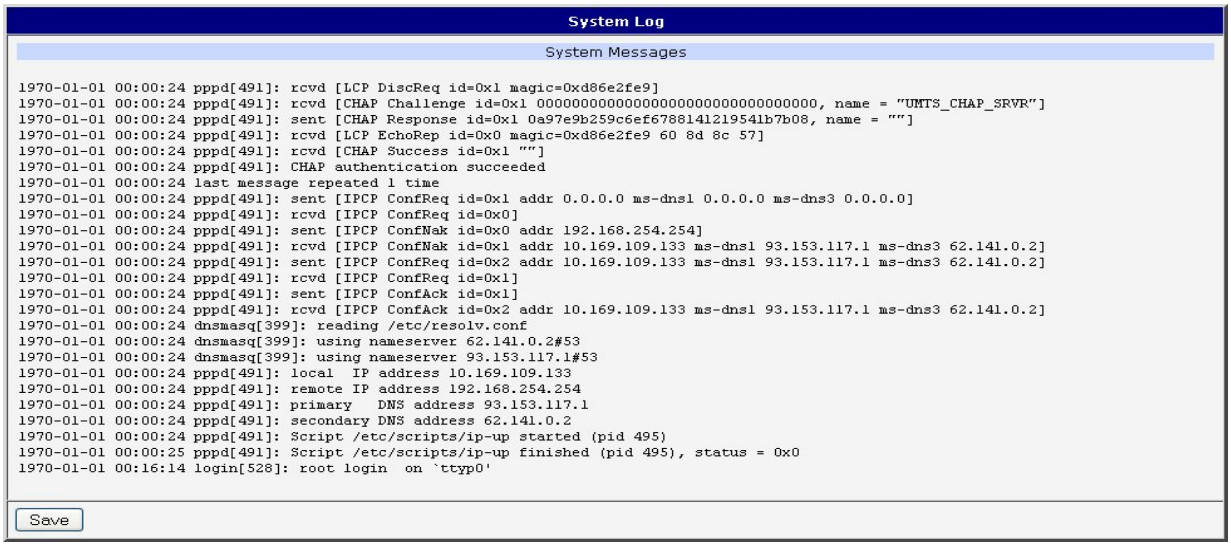


Fig. 7: System log

The Syslog default size is 1000 lines. After completion of the 1000 lines will create new file for storing system log. After completion of the 1000 lines in the second file, the first file is deleted and creates a new one.

Program syslogd can be started with two options that modifies its behavior. Option "-s" followed by decimal number set maximal number of lines in one log file. Option "-r" followed by hostname or IP address enable logging to remote syslog daemon.

In the Linux must be enabled remote logging on the target computer. Typically running syslogd with the parameter “-r”. On Windows must be installed the syslog server (for example Syslog Watcher).

For starting syslogd with these options you could modify script "/etc/init.d/syslog" or add lines "killall syslogd" and "syslogd <options> &" into Startup Script.

Example of logging into the remote daemon at 192.168.2.115

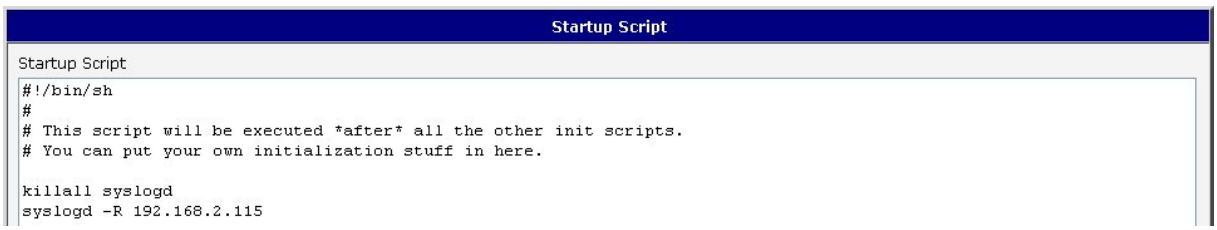


Fig. 8: Example program syslogd start with the parameter -r

1.8. *LAN configuration*

To enter the network configuration, select the ***LAN*** menu item. ETH network set in ***Primary LAN*** configuration, expansion PORT ETH set in ***Secondary LAN*** configuration.

Item	Description
DHCP Client	• disabled – The router does not allow automatic allocation IP address from a DHCP server in LAN network. • enabled – The router allows automatic allocation IP address from a DHCP server in LAN network.
IP address	Fixed set IP address of network interface ETH.
Subnet Mask	IP address of Subnet Mask.
Media type	• Auto-negation – The router selects the speed of communication of network options. • 100 Mbps Full Duplex – The router communicates at 100Mbps, in the full duplex mode. • 100 Mbps Half Duplex - The router communicates at 100Mbps, in the half duplex mode. • 10 Mbps Full Duplex - The router communicates at 10Mbps, in the full duplex mode. • 10 Mbps Half Duplex - The router communicates at 10Mbps, in the half duplex mode.
Default Gateway	IP address of Default gateway of router. When entering IP address of default gateway, all packets for which the record was not found in the routing table, sent to this address.
DNS server	IP address of DNS server of router. Address where they are forwarded to all DNS questions on the router.

Table 9: Configuration of network interface

DHCP server assigns IP address, gateway IP address (IP address of the router) and IP address of the DNS server (IP address of the router) to the connected clients.

DHCP server supports static and dynamic assignment of IP addresses. Dynamic DHCP server assigns clients IP addresses from a defined address space. Static DHCP assigns IP addresses that correspond to the MAC addresses of connected clients.

Item	Description
Enable dynamic DHCP leases	If this option is checked, can enable a dynamic DHCP server.
IP Pool Start	Start IP addresses space to be allocated to the DHCP clients.
IP Pool End	End IP addresses space to be allocated to the DHCP clients.
Lease time	Time in seconds, after which the client can use IP address.

Table 10: Configuration of dynamic DHCP server

Item	Description
Enable static DHCP leases	If this option is checked, can enable a static DHCP server.
MAC Address	MAC address of a DHCP client.
IP Address	Assigned IP address.

Table 11: Configuration of static DHCP server

It is important not to overlap ranges of static allocated IP address with address allocated by the dynamic DHCP. Then risk collision of IP addresses and incorrect function of network.

Example of the network interface with dynamic DHCP server:

- The range of dynamic allocated addresses from 192.168.1.2 to 192.168.1.4.
- The address is allocated 600 second (10 minutes).

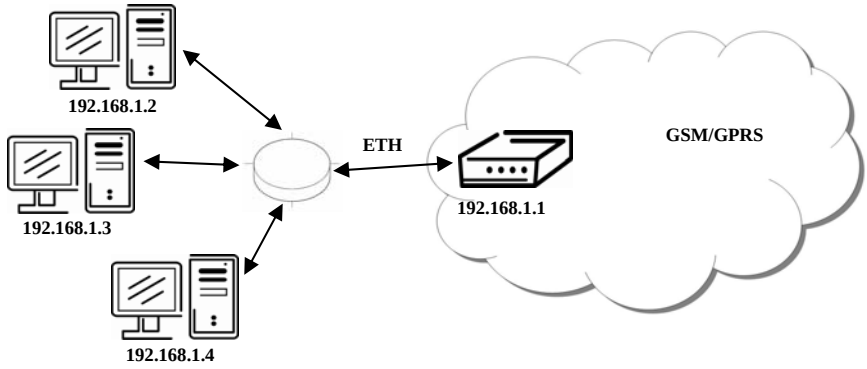


Fig. 9: Topology of example LAN configuration 1

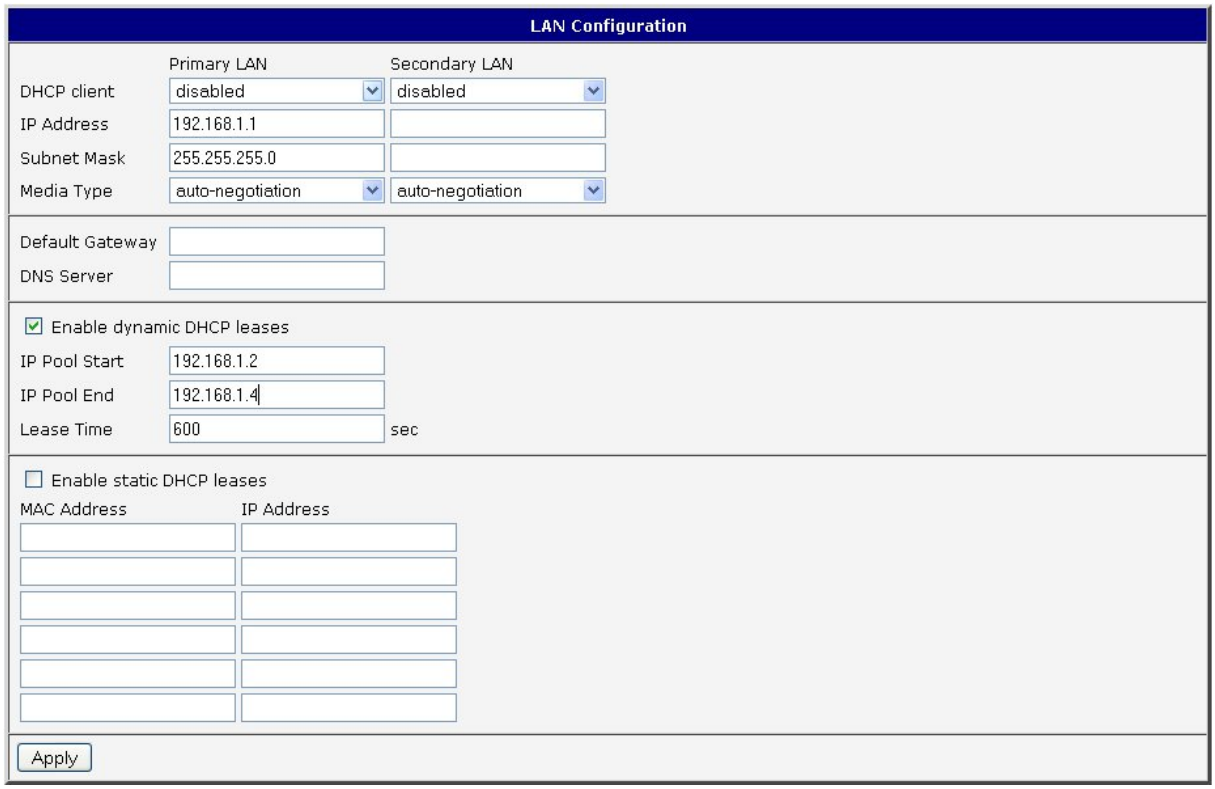


Fig. 10: Example LAN configuration 1

Example of the network interface with dynamic and static DHCP server:

- The range of allocated addresses from 192.168.1.2 to 192.168.1.4.
- The address is allocated 10 minutes.
- Client's with MAC address 01:23:45:67:89:ab has IP address 192.168.1.10.
- Client's with MAC address 01:54:68:18:ba:7e has IP address 192.168.1.11.

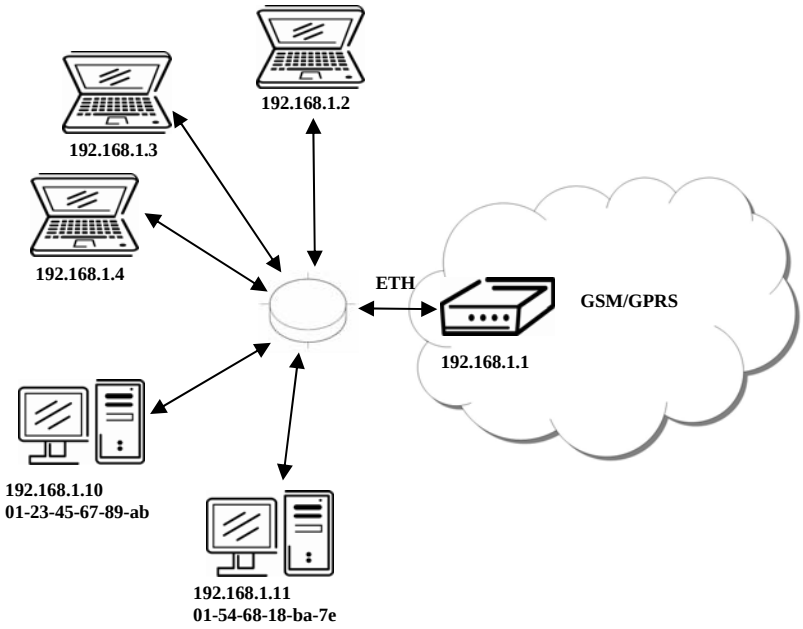


Fig. 11: Topology of example LAN configuration 2

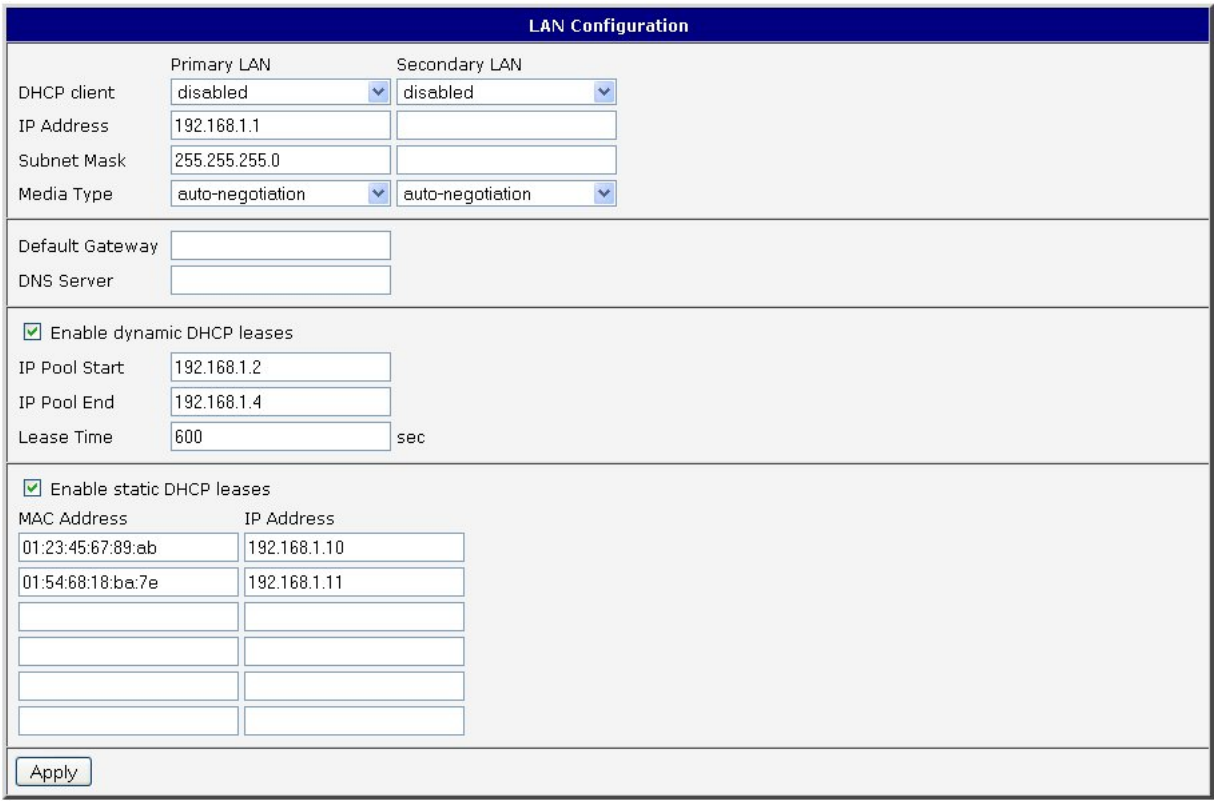


Fig. 12: Example LAN configuration 2

Example of the network interface with default gateway and DNS server:

- Default gateway IP address is 192.168.1.20
- DNS server IP address is 192.168.1.20

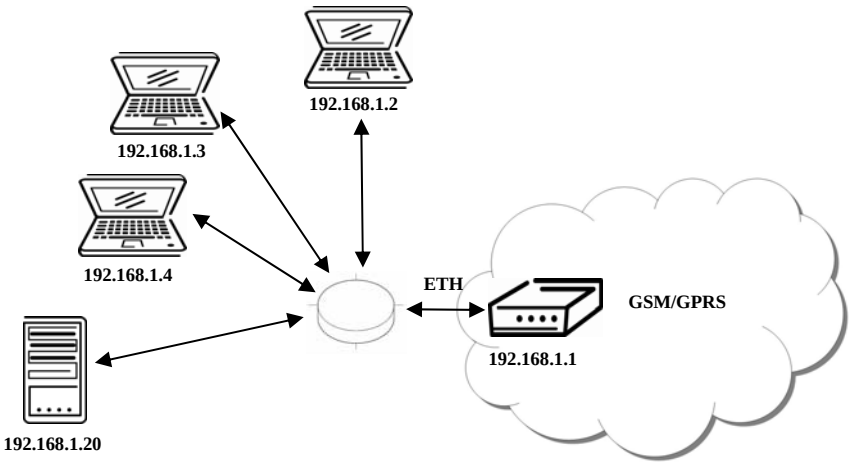


Fig. 13: Topology of example LAN configuration 3

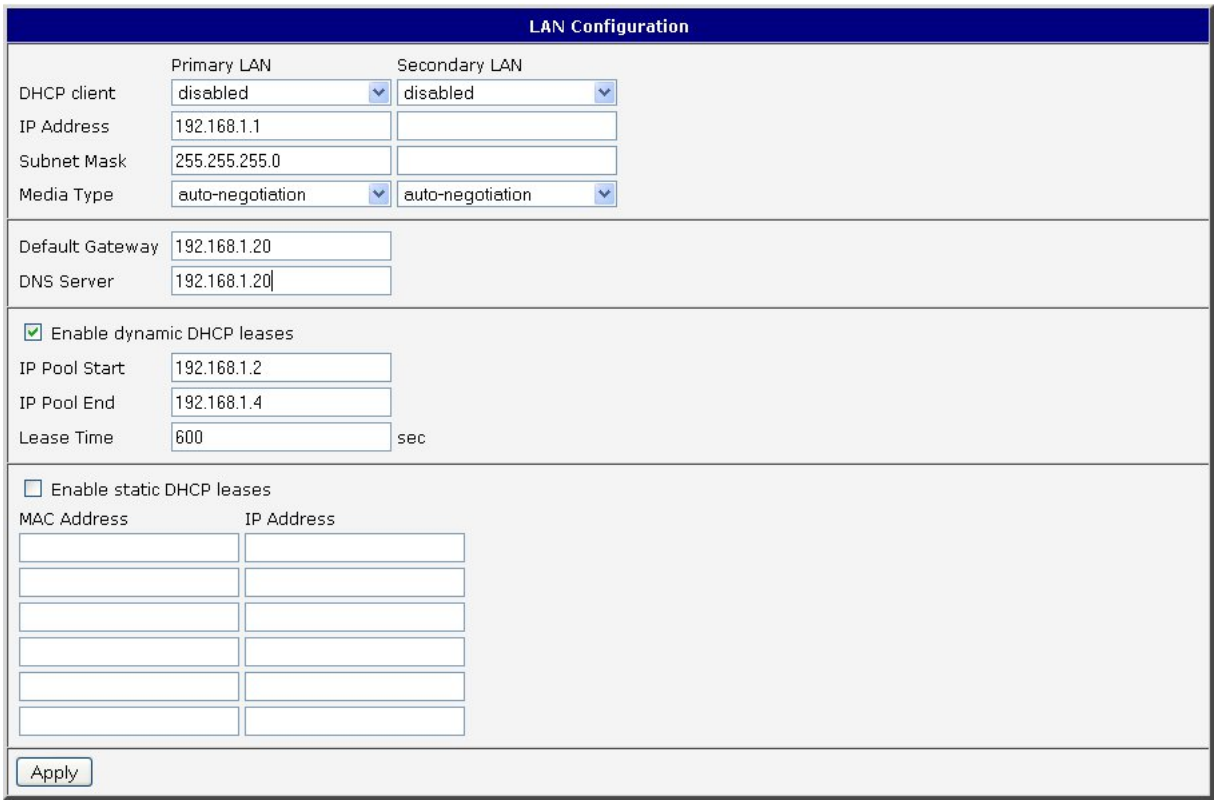


Fig. 14: Example LAN configuration 3

1.9. *VRRP configuration*

To enter the VRRP configuration select the ***VRRP*** menu item. VRRP protocol (Virtual Router Redundancy Protocol) is a technique, by which it is possible to forward routing from main router to backup router in the case of the main router failure. If the ***Enable VRRP*** is checked, then it is possible to set the following parameters.

Item	Description
Virtual Server IP Address	This parameter sets virtual server IP address. This address should be the same for both routers. A connected device sends its data via this virtual address.
Virtual Server ID	Parameter *Virtual Server ID* distinguishes one virtual router on the network from others. Main and backup routers must use the same value for this parameter.
Host Priority	The router, with higher priority set by the parameter *Host Priority*, is the main router. According to RFC 2338 the main router has the highest possible priority - 255. The backup router has priority in range 1 – 254 (init value is 100). The priority value equals 0 is not allowed.

Table 12: VRRP configuration

It is possible to set ***Check PPP connection*** flag in the second part of the window. The currently active router (main/backup) will send testing messages to defined *Ping IP Address* at periodic time intervals (*Ping Interval)* with setting time of waiting for answer (*Ping Timeout)*. The function check PPP connection is used as a supplement of VRRP standard with the same final result. If there are no answers from remote devices (*Ping IP Address*) for a defined number of probes (*Ping Probes),* then connection is switched to the other line.

Item	Description
Ping IP Address	Destinations IP address ping queries. Address can not specify as domain name.
Ping Interval	Time intervals between the outgoing pings.
Ping Timeout	Time to wait to answer.
Ping Probes	Number of failed ping requests, after which the route is considered to be impassable.

Table 13: Check PPP connection

Ping IP address is possible to use for example a DNS server of mobile operator as a test message (ping) IP address.

There's an additional way for evaluating the state of the active line. It is activated by selecting ***Enable traffic monitoring*** parameter. If this parameter is set and any packet different from ping is sent to the monitored line, then any answer to this packet is expected for *Ping Timeout*. If *Ping Timeout* expires with no answer received then process of testing the active line continues the same way like in the case of standard testing process after first test message answer drops out.

Example of the VRRP protocol:

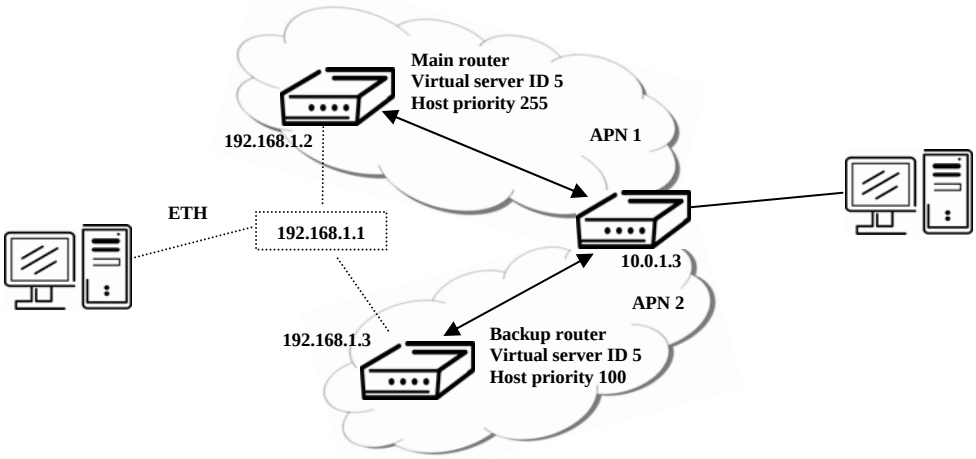


Fig. 15: Topology of example VRRP configuration

VRRP Configuration

Enable VRRP	
Virtual Server IP Address	192.168.1.1
Virtual Server ID	5
Host Priority	255
Check PPP connection	
Ping IP Address	10.0.1.3
Ping Interval	10 sec
Ping Timout	5 sec
Ping Probes	10
Enable traffic monitoring	

Apply

Fig. 16: Example VRRP configuration – main router

VRRP Configuration

Enable VRRP	
Virtual Server IP Address	192.168.1.1
Virtual Server ID	5
Host Priority	100
Check PPP connection	
Ping IP Address	10.0.1.3
Ping Interval	10 sec
Ping Timout	5 sec
Ping Probes	10
Enable traffic monitoring	

Apply

Fig. 17: Example VRRP configuration – backup router

1.10. *GPRS configuration*

The industrial router XR5i v2 is not availability item GPRS Configuration.

To enter the GPRS connection configuration select the ***GPRS*** menu item.

1.10.1. GPRS connection

If the **Create GPRS connection** option is selected, the modem automatically tries to establish GPRS connection after switching-on.

Item	Description
APN	Network identifier (Access Point Name)
Username	User name to log into the GSM network.
Password	Password to log into the GSM network.
Authentication	Authentication protocol in GSM network • PAP or CHAP – Router is chosen one of the authentication methods. • PAP – It is used PAP authentication method. • CHAP – It is used CHAP authentication method.
IP Address	IP address of SIM card. The user sets the IP address, only in the case IP address was assigned of the operator.
Phone Number	Telephone number to dial GPRS or CSD connection. Router as a default telephone number used *99***1 #.
Operator	This item can be defined PLNM preferred carrier code
Network type	• Automatic selection – The router automatically selects a specific transmission method according to the availability of transmission technology. • Furthermore, according to the type of router - it is also possible to select a specific method of data transmission (GPRS, EDGE, UMTS …).
PIN	PIN parameter should be set only if it requires a SIM card router. SIM card is blocked in case of several bad attempts to enter the PIN.
MRU	Maximum Receiving Unit) – it is the identifier of the maximum size of packet, which is possible to receive in a given environment. Default value is 1500 bytes. Other settings may cause incorrect transmission of data.
MTU	(Maximum Transmission Unit) – it is the identifier of the maximum size of packet, which is possible to transfer in a given environment. Default value is 1500 bytes. Other settings may cause incorrect transmission of data.

Table 14: GPRS connection configuration

If the *IP address* field is not filled in, the operator automatically assigns the IP address when it is establishing the connection. If filled IP address supplied by the operator, router accelerate access to the network.

If the *APN* field is not filled in, the router automatically selects the APN by the IMSI code of the SIM card. If the PLMN (operator number format) is not in the list of APN, then default APN is “internet“. The mobile operator defines APN.

If only one SIM card is plugged in the router, router switches between the APN. Router with two SIM cards switches between SIM cards.

Correct PIN must be filled. For SIM cards with two APN's there will be the same PIN for both APN`s. Otherwise the SIM card can be blocked by false SIM PIN.

Items marked with an asterisk must be filled only if the information required by the operator.

In the case of a failed build a PPP connection is recommended to check the accuracy of entered data. Alternatively, try a different authentication method or network type.

1.10.2. DNS address configuration

The choice ***Get DNS address from operator*** is given for easier configuration on client side. If this field is filled in, then the router tries to get an IP address of primary and secondary DNS server from the operator automatically.

1.10.3. Check PPP connection configuration

If the ***Check PPP connection*** option is selected, it has active control of connection over PPP. The modem will automatically send the ping question to the selected domain name or IP address in periodic time intervals. If the PING failed, new ping be sent immediately. After three unsuccessfully pings on appropriate IP address the router terminates connection and tries to establish a new connection. It is possible to use, for example, the DNS server of a mobile operator as the ping IP address.

Item	Description
Ping IP Address	Destinations IP address or domain name of ping queries.
Ping Interval	Time intervals between the outgoing pings.

Table 15: Check PPP connection configuration

If the ***Enable Traffic Monitoring*** option is selected, then the router stops sending ping questions to the *Ping IP Address* and it will watch traffic in PPP connection. If PPP connection is without traffic longer than the *Ping Interval,* then the router sends ping questions to the Ping IP Address.

Attention! We recommend checking the GPRS connection in case of uninterrupted running.

1.10.4. Data limit configuration

Item	Description
Data limit	With this parameter you can set the maximum expected amount of data transmitted (sent and received) over GPRS in one billing period (month).
Warning Threshold	Parameter *Warning Threshold* determine per cent of *Data Limit* in the range of 50% to 99%, which if is exceeded, then the router sends SMS in the form *Router has exceeded (value of Warning Threshold) o data limit*.
Accounting Start	Parameter sets the day of the month in which the billing cycle starts SIM card used. Start of the billing period defines the operator, which gives the SIM card. The router begin to count the transferred data since that day

Table 16: Data limit configuration

If the parameter *Switch to backup SIM card when data limit is exceeded* (see next) or *Send SMS when datalimit is exceeded* (see SMS configuration) are not selected the data limit will not count.

1.10.5. Switch between SIM cards configuration

At the bottom of configuration it is possible to set rules for switching between two APN's on the SIM card, in the event that one SIM card is inserted or between two SIM cards, in the event that two SIM cards are inserted.

Item	Description
Default SIM card	This parameter sets default APN or SIM card, from which it will try to establish the PPP connection. If this parameter is set to *none,* the router launches in off-line mode and it is necessary to establish PPP connection via SMS message.
Backup SIM card	Defines backup APN or SIM card, that the router will switch the defining one of the following rules.

Table 17: Default and backup SIM configuration

If parameter Backup SIM card is set to none, then parameters *Switch to other SIM card when connection fails, Switch to backup SIM card when roaming is detected and Switch to backup SIM card when data limit is exceeded* switch the router to off-line mode.

Item	Description
Switch to other SIM card when connection fails	If PPP connection fails, then this parameter ensures switch to secondary SIM card or secondary APN of the SIM card. Failure of the PPP connection can occur in two ways. When I start the router, when three fails to establish a PPP connection. Or if it is checked Check the PPP connection, and is indicated by the loss of a PPP connection.
Switch to backup SIM card when roaming is detected	In case that the roaming is detected this parameter enables switching to secondary SIM card or secondary APN of the SIM card.
Switch to backup SIM card when data limit is exceeded	This parameter enables switching to secondary SIM card or secondary APN of the SIM card, when the data limit of default APN is exceeded.
Switch to backup SIM card when binary input is active	This parameter enables switching to secondary SIM card or secondary APN of the SIM card, when binary input 'bin0' is active.
Switch to primary SIM card after timeout	This parameter defines the method, how the router will try to switch back to default SIM card or default APN.

Table 18: Switch between SIM card configurations

The following parameters define the time after which the router attempts to go back to the default SIM card or APN.

Item	Description
Initial timeout	The first attempt to switch back to the primary SIM card or APN shall be made for the time defined in the parameter Initial Timeout, range of this parameter is from 1 to 10000 minutes.
Subsequent Timeout	In an unsuccessful attempt to switch to default SIM card, the router on the second attempt to try for the time defined in the parameter Subsequent Timeout, range is from 1 to 10000 minutes.
Additive constants	Any further attempt to switch back to the primary SIM card or APN shall be made in time computed as the sum of the previous time trial and time defined in the parameter Additive constants range is 1-10000 minutes.

Table 19: Switch between SIM card configurations

Example: If parameter *Switch to primary SIM card after timeout* is checked and parameters are set as follows *Initial Timeout* – 60min. *Subsequent Timeout* 30min a *Subsequent Timeout* - 20min.The first attempt to switch the primary SIM card or APN shall be carried out after 60 minutes. Switched to a failed second attempt made after 30 minutes. Third after 50 minutes (30 +20). Fourth after 70 minutes (30 +20 +20).

1.10.6. Dial-In access configuration

Dial in access configuration is supported only for routers ER75i, UR5, ER75i v2 UR5 v2 and v2.

In the bottom part of the window it is possible to define access over CSD connection by *Enable Dial-In Access* function. Access can be secured by used the *Username* and *Password*. In the event that this function is enabled and the router does not have a PPP connection is granted access to the router via dial-up connections CSD. The router waits 2 minutes to accept connections. If the router during this time nobody logs on, the router will try again to establish a GPRS connection.

Item	Description
Username	User name for secured Dial-In access.
Password	Password for secured Dial-In access.

Table 20: Dial-In access configuration

1.10.7. PPPoE bridge mode configuration

If the *Enable* ***PPPoE bridge mode*** option selected, it activate the PPPoE bridge protocol PPPoE (point-to-point over ethernet) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. Allows you to create a PPPoE connection from the device behind router. For example from PC which is connected to ETH port router. There will be allot Ip address of SIM card to PC.

The changes in settings will apply after pressing the *Apply* button.

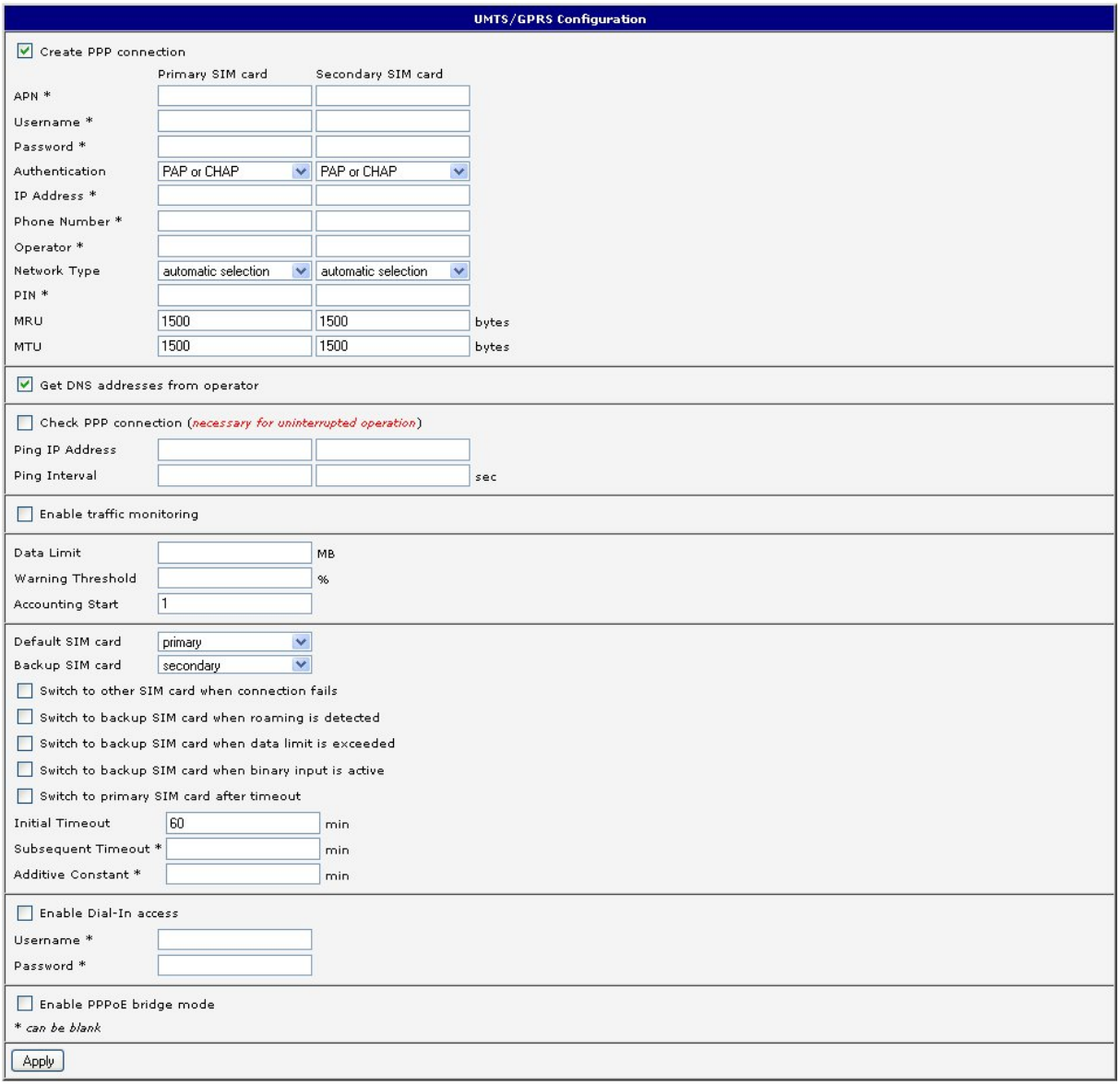


Fig. 18: GPRS configuration

Example of setting controls the PPP connection to the address 8.8.8.8 in the time interval of 60s for primary SIM card and to the address www.google.com in the time interval 80s for secondary SIM card. In the case of traffic on the PPP control pings are not sent, but the traffic on PPP is observed:

Fig. 19: Example of GPRS configuration 1

Example of switching to a backup SIM card after exceeding the data limits of 800MB Sending SMS warning when reaching 400MB. With the beginning billing day of the 18th of the month:

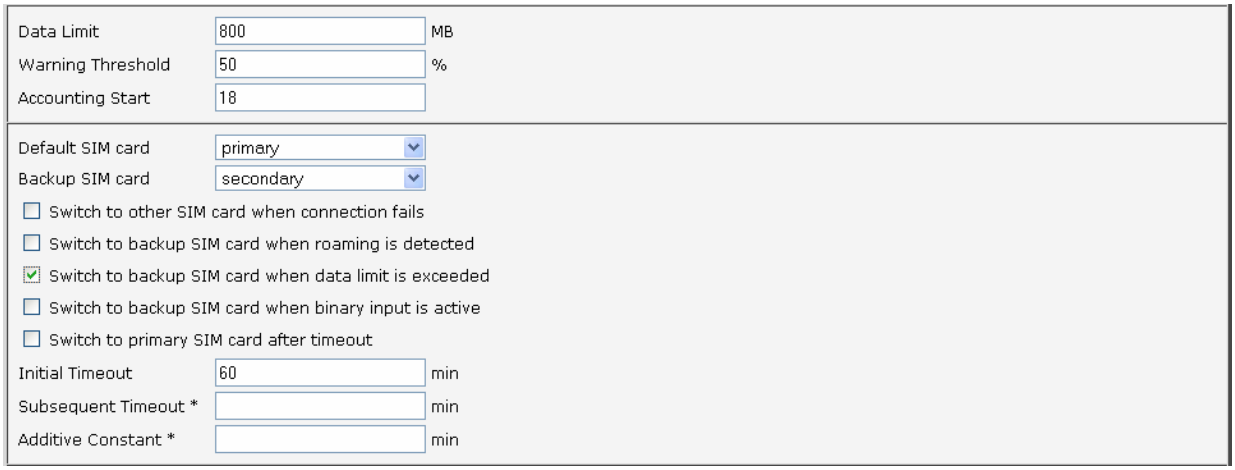


Fig. 20: Example of GPRS configuration 2

Example: Primary SIM card switch to offline modes, after router detection roaming. The first attempt to switch back to the default SIM card is done after 60 minutes, the second after 40 minutes, the third after 50 minutes (40 +10)...

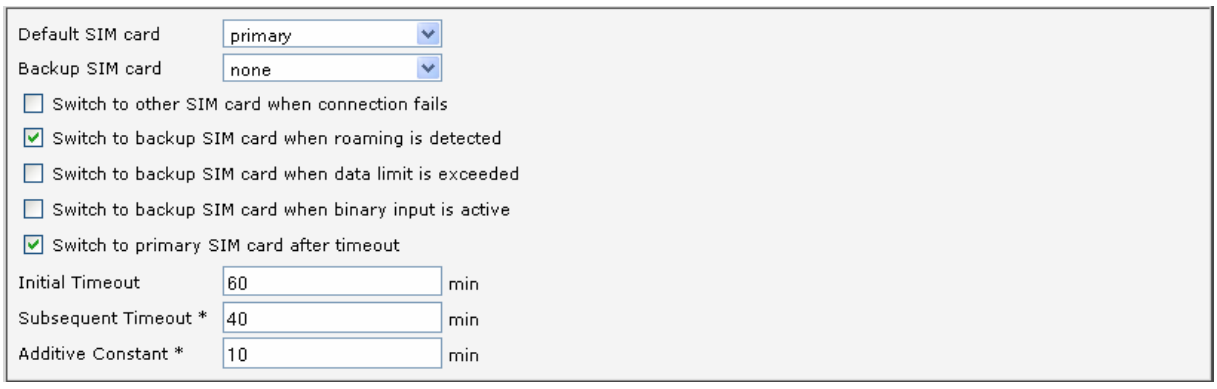


Fig. 21: Example of GPRS configuration 3

1.11. *PPPoE configuration*

PPPoE configuration item is available only on the industrial router XR5i v2.

PPPoE for industrial router works in client mode. Router using connection to the PPPoE server or PPPoE bridge (for example ADSL modem).

To enter the PPPoE configuration select the ***PPPoE*** menu item. If the *Create PPPoE connection* option is selected, the router tries to establish PPPoE connection after switching-on. PPPoE (Point-to-Point over Ethernet) is a network protocol, which PPP frames encapsulating to the Ethernet frames. PPPoE client to connect devices that support PPPoE bridge or a server (typically ADSL router). After connecting the router obtains the IP address of the device to which it is connected. All communications from the device behind the PPPoE server is forwarded to industrial router.

Item	Description
Username	Username for secure access to PPPoE
Password	Password for secure access to PPPoE
Authentication	Authentication protocol in GSM network • PAP or CHAP – Router is chosen one of the authentication methods. • PAP – It is used PAP authentication method. • CHAP – It is used CHAP authentication method.
MRU	(Maximum Receiving Unit) – it is the identifier of the maximum size of packet, which is possible to recese in given environment. Default value is set to 1492 bytes. Other settings may cause incorrect data transmission.
MTU	(Maximum Transmission Unit) – it is the identifier of the maximum size of packet, which is possible to transfer in given environment. Default value is set to 1492 bytes. Other settings may cause incorrect data transmission.

Table 21: PPPoE configuration

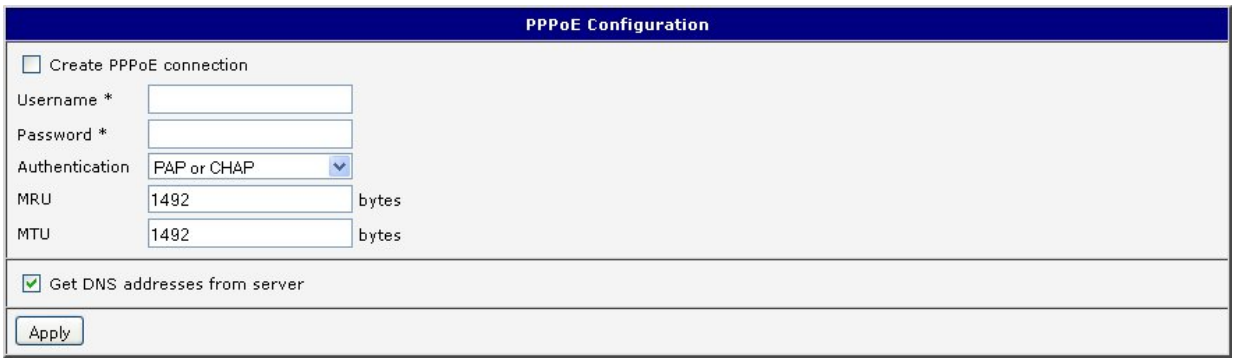


Fig. 22: PPPoE configuration

1.12. *Firewall configuration*

By the help of a firewall it is possible to set IP addresses from which are possible to remotely access the router and internal network connected behind a router. The choice ***Allow remote access only from specified hosts*** is given for easier configuration of hosts. In this firewall configuration it is possible to set up to four remote accesses by the help of *Source*, *Source IP Address*, *Protocol* and *Target Port*.

Item	Description
Source	• single address - access allowed a single IP address defined in the Source IP Address • any address – allowed access to any IP address
Source IP address	IP address from which it is allowed to access the router.
Protocol	Specify protocol for remote access • all – access is allowed by all • TCP – access is allowed by TCP • UDP - access is allowed by UDP • ICMP access is allowed by ICMP
Target Port	The port number on which it is allowed to access the router.

Table 22: Firewall configuration

Caution! Firewall doesn't filter via Ethernet.

Example of the firewall configuration:

The router has allowed the following access:

- from address 171.92.5.45 using any protocol
- from address 10.0.2.123 using TCP protocol on any ports
- from address 142.2.26.54 using ICMP protocol

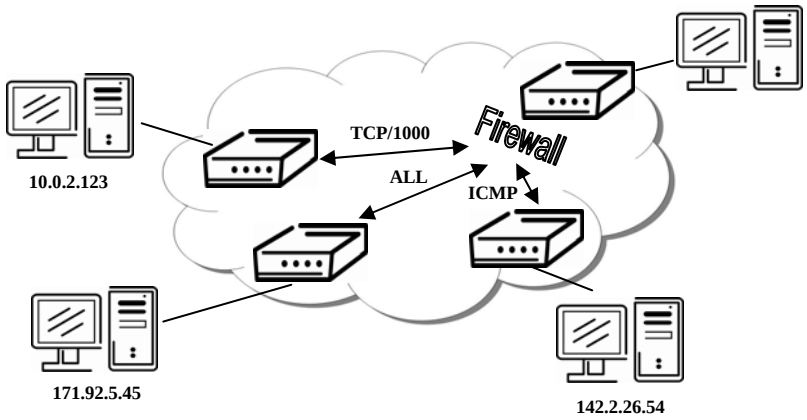


Fig. 23: Topology of example firewall configuration

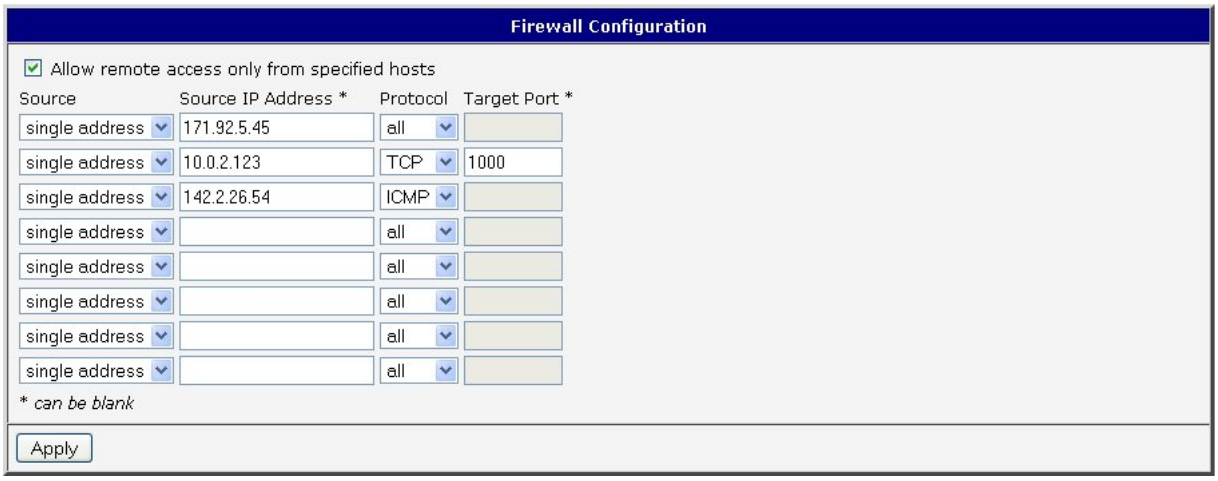


Fig. 24: Example firewall configuration

1.13. *NAT configuration*

To enter the Network Address Translation configuration, select the ***NAT*** menu item. NAT (Network address Translation / Port address Translation - PAT) is a method of adjusting the network traffic through the router default transcript and/or destination IP addresses often change the number of TCP/UDP port for walk-through IP packets. The window contains sixteen entries for the definition of NAT rules.

Item	Description
Public Port	Public port
Private Port	Private port
Type	Protocol selection
Server IP address	IP address which will be forwarded incoming data.

Table 23: NAT configuration

If necessary set more than sixteen rules for NAT rules, then is possible insert into start up script following script:

iptables -t nat -A napt -p tcp --dport [PORT_PUBLIC] -j DNAT --to-destination [IPADDR]:[PORT1_PRIVATE], Concrete IP address [IPADDR] and ports numbers [PORT_PUBLIC] and [PORT1_PRIVATE] are filled up into square bracket.

Reconfiguration of PPPoE, Firewall, NAT, OpenVPN, IPsec, Expansion Port and USB Port always leads to restarting IPtables. In case that someone has additional rules in Startup Script then reboot of router is needed.

The following items are used to set the routing of all incoming traffic from the PPP to the connected computer.

Item	Description
Send all incoming packets to default server	By checking this item and setting the *Default Server* item it is possible to put the router into the mode in which all incoming data from GPRS will be routed to the computer with the defined IP address.
Default Server	Send all incoming packets to this IP addresses.

Table 24: Configuration of send all incoming packets

Enable the following options and enter the port number is allowed remote access to the router from PPP interface.

Item	Description
Enable remote HTTP access on port	If this item field and port number is filled in, then configuration of the router over web interface is possible.
Enable remote HTTPS access on port	If this item field and port number is filled in, then configuration of the router over web interface is possible.
Enable remote FTP access on port	Choice this item and port number makes it possible to access over *FTP*.
Enable remote SSH access on port	Choice this item and port number makes it possible to access over SSH.
Enable remote Telnet access on port	Choice this item and port number makes it possible to access over Telnet.
Enable remote SNMP access on port	Choice this item and port number makes it possible to access to SNMP agent.
Masquerade outgoing packets	Choice Masquerade (alternative name for the NAT system) item option turns the system address translation NAT.

Table 25: Remote access configuration

Example of the configuration with one connection equipment on the router:

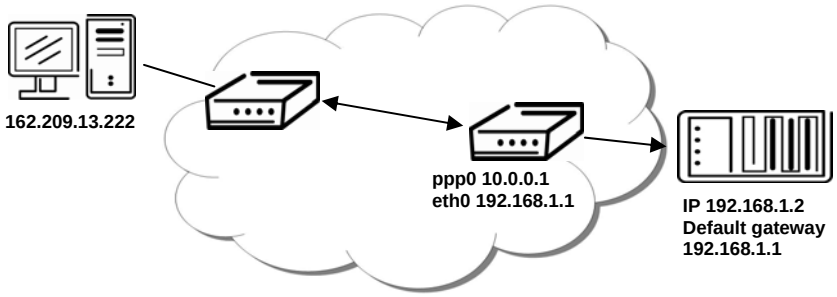


Fig. 25: Topology of example NAT configuration

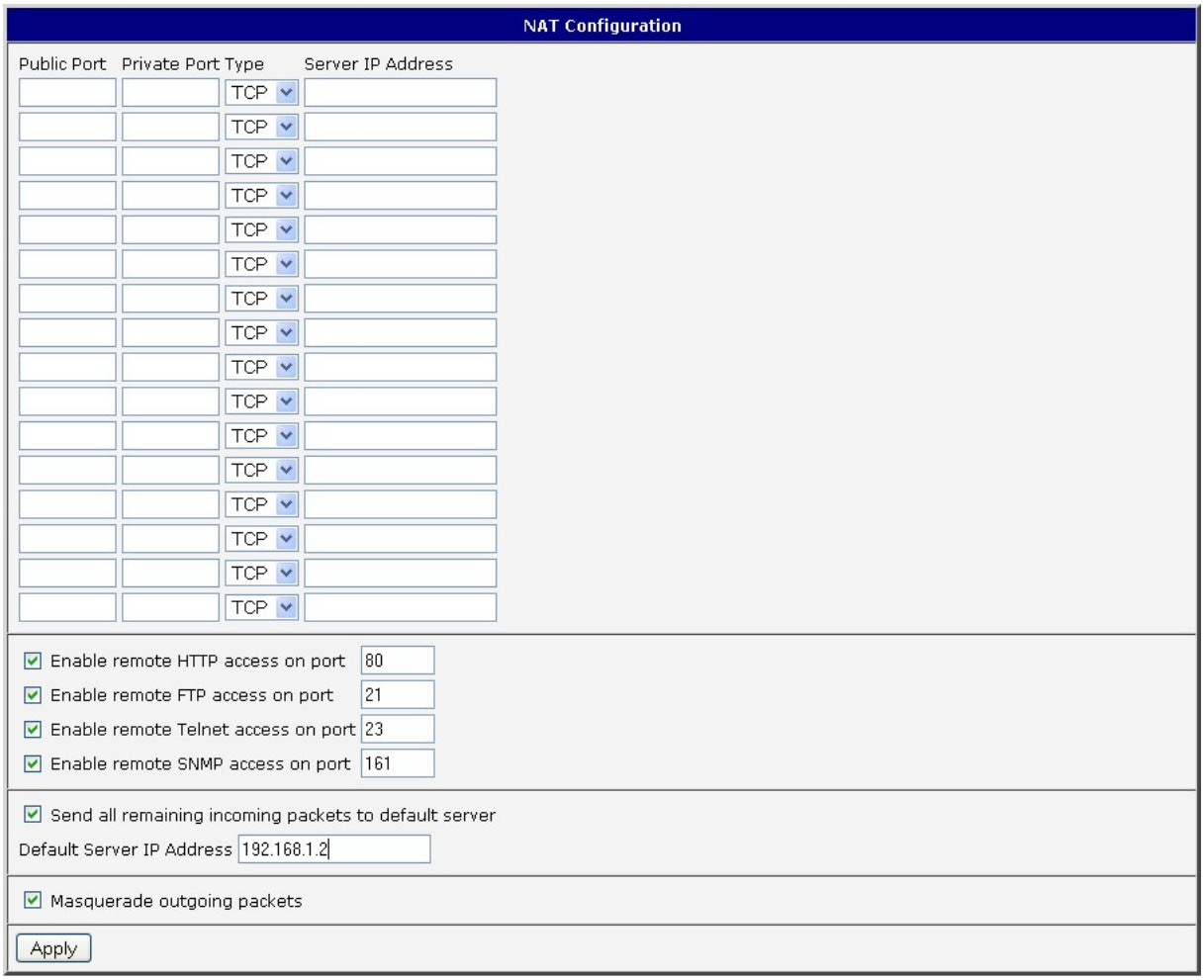


Fig. 26: Example NAT configuration 1

In these configurations it is important to have marked choice of *Send all remaining incoming packets it default server*, IP address in this case is the address of the device behind the router. Connected equipment behind the router must have set **Default Gateway** on the router. Connected device replies, while PING on IP address of SIM card.

Example of the configuration with more connected equipment:

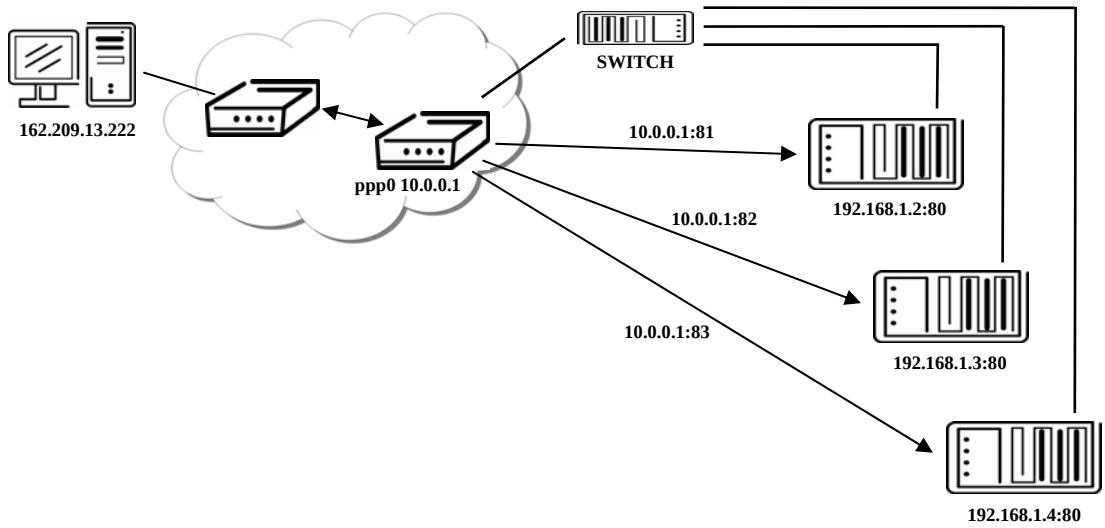


Fig. 27: Topology of example NAT configuration

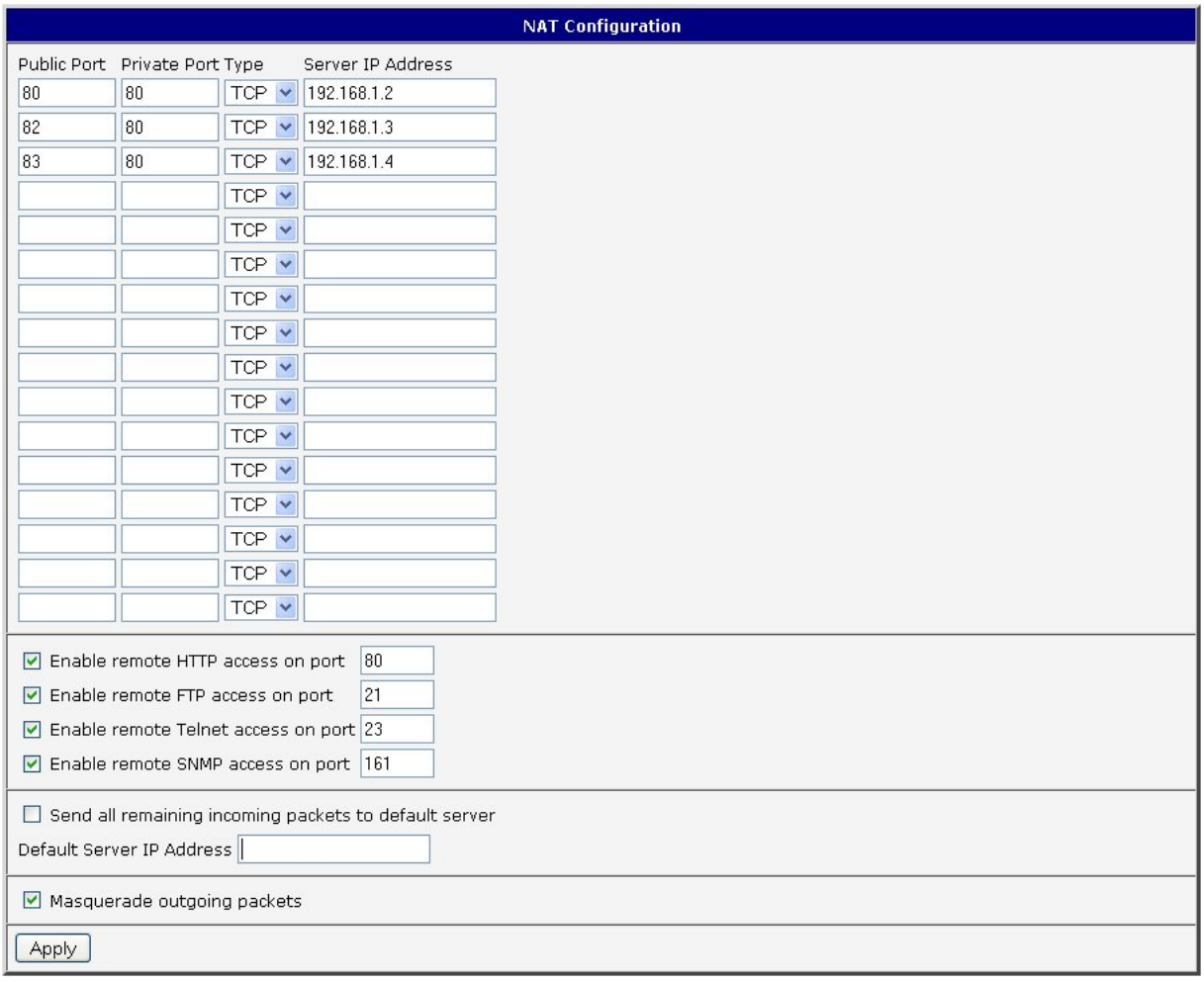


Fig. 28: Example of NAT configuration 2

In this configuration equipment wired behind the router defines the address *Server IP Address*. The router replies, while PING on address of SIM card. Access on web interface of the equipment behind the router is possible by the help of Port Forwarding, when behind IP address of SIM is indicating public port of equipment on which we want to come up. At demand on port 80 it is surveyed singles outer ports (Public port), there this port isn't defined, therefore at check selection Enable remote http access it automatically opens the web interface router. If this choice isn't selected and is selected volition Send all remaining incoming packets to the default server fulfill oneself connection on induction IP address. If it is not selected selection *Send all remaining incoming packets to default server* and *Default server IP address* then connection requests a failure.

1.14. *OpenVPN tunnel configuration*

OpenVPN tunnel configuration can be called up by option ***OpenVPN*** item in the menu. OpenVPN tunnel allows protected connection of two networks LAN to the one which looks like one homogenous. In the **OpenVPN Tunnels Configuration** window are two rows, each row for one configured OpenVPN tunnel.

Item	Description
Create	This item enables the individual tunnels.
Description	This item displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Configuration OpenVPN tunnel.

Table 26: Overview OpenVPN tunnels

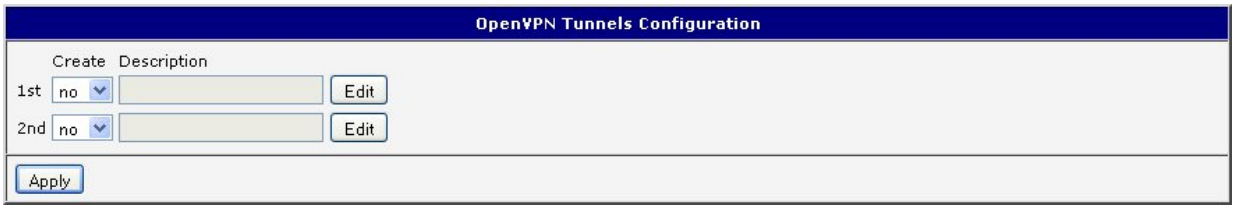


Fig. 29: OpenVPN tunnels configuration

Item	Description
Description	Description of tunnel.
Protocol	Protocol, by which the tunnel will communicate. • **UDP** – OpenVPN will communicate using UDP. • **TCP server** – OpenVPN will communicate using TCP in server mode. • **TCP client** – OpenVPN will communicate using TCP in client mode.
UDP/TCP port	Port, by which the tunnel will communicate.
Remote IP Address	IP address of the opposite side of the tunnel. Can be used domain name.
Remote Subnet	Network IP address of the opposite side of the tunnel.
Remote Subnet Mask	Subnet mask of the opposite side of the tunnel.
Redirect Gateway	By this parameter is possible to redirect all traffic on Ethernet.
Local Interface IP Address	IP address of the local side of tunnel.

Remote Interface IP Address	IP address of interface local side of tunnel.
Ping Interval	This parameter defines the time period after which router sends a message to opposite side of tunnel, for check the existence of the tunnel.
Ping Timeout	*Ping Timeout* waits on message from off-side tunnel. For OpenVPN tunnel right verifies parameter *Ping Timeout* has to be bigger than *Ping Interval*.
Renegotiate Interval	This parameter sets renegotiate period (reauthorization) of the OpenVPN tunnel. This parameter is possible to set only at username/password authentication or at X.509 certificate using. After this time period, the router changes the encryption tunnel to ensure the continued safety of the tunnel.
Max Fragment Size	By parameter *Max Fragment Size* it is possible to define maximum sending packet size.
Compression	Sending data is possible compress • **none** – No compression is used. • **LZO** – Are used lossless LZO compressions. Compression has to be on both tunnel ends.
NAT Rules	By parameter NAT Rules it is possible to apply set NAT rules to OpenVPN tunnel. • **not applied** – NAT rules to OpenVPN is not applied. • **applied** – NAT rules to OpenVPN is applied.
Authenticate Mode	This parameter can be set authentication mode. • **none** – is used any authentication mode • **Pre-shared secret** – enables authentication using Pre-shared secret. This authentication set shared key for both off-side tunnel • **Username/password** – enables authentication using CA Certificate, Username and Password • **X.509 Certificate (multiclient)** – enables authentication by *CA Certificate*, *Local Certificate* and *Local Private Key* • **X.509 Certificate (client)** – enables authentication by *CA Certificate*, *Local Certificate* and *Local Private Key* • **X.509 Certificate (server)** - enables authentication by *CA Certificate*, *Local Certificate* and *Local Private Key*
Pre-shared Secret	Authentication using Pre-shared secret can be used in all offered authentication mode.
CA Certificate	This authentication certificate can be used in authentication mode Username/password and X.509 certificate.
DH Parameters	Protocol for exchange key DH parameters can be used in authentication mode X.509 server.
Local Certificate	This authentication certificate can be used in authentication mode X.509 certificate.
Local Private Key	Local private key can be used in authentication mode X.509 certificate.
Username Password	Authentication using a login name and password authentication can be used in the Authenticate Mode Username/Password.

Extra Options	By the help of parameter *Extra Options* it is possible to define additional parameters of the OpenVPN tunnel, for example DHCP options etc.

Table 27: OpenVPN configuration

The changes in settings will apply after pressing the *Apply* button.

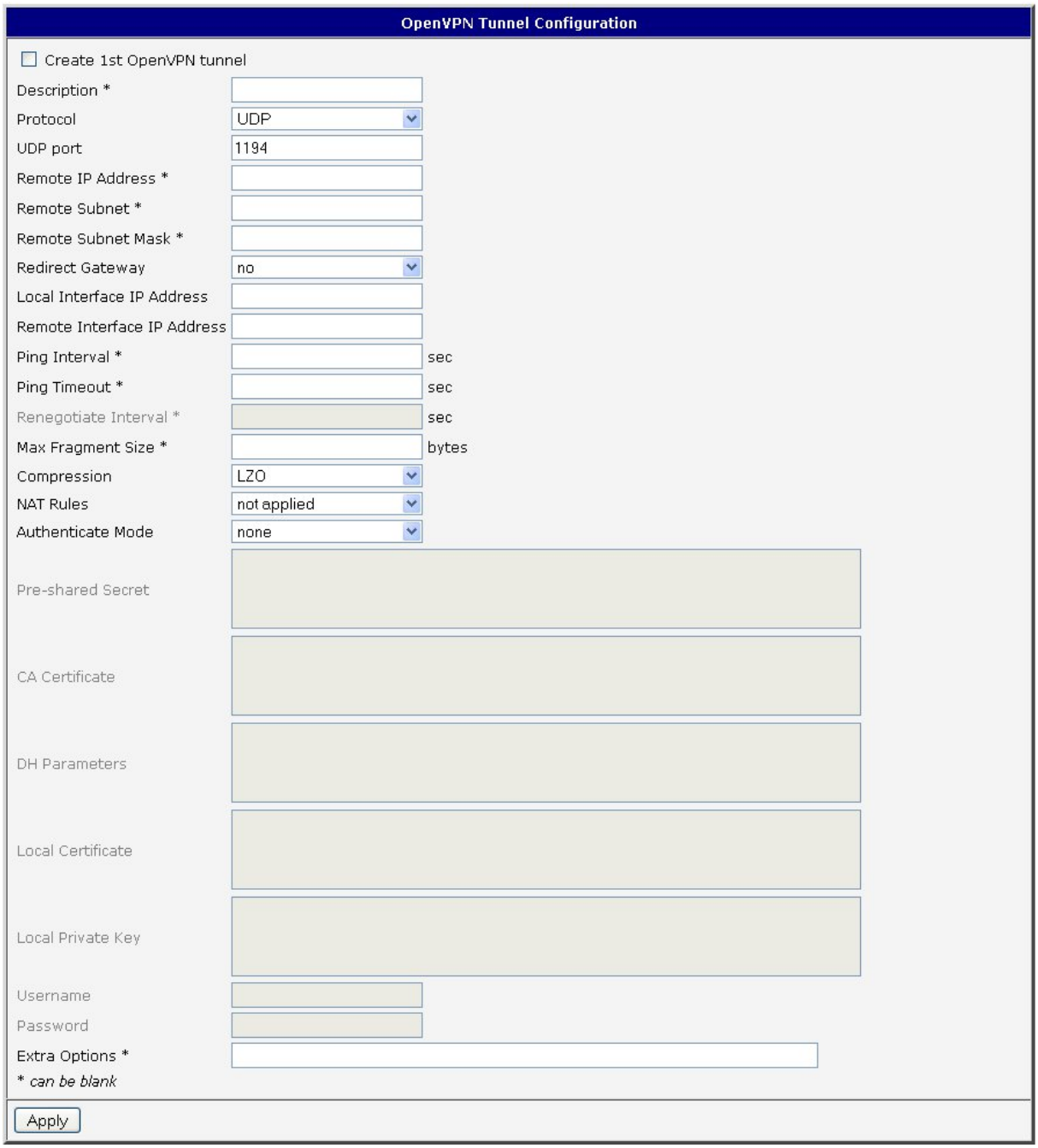


Fig. 30: OpenVPN tunnel configuration

Example of the OpenVPN tunnel configuration:

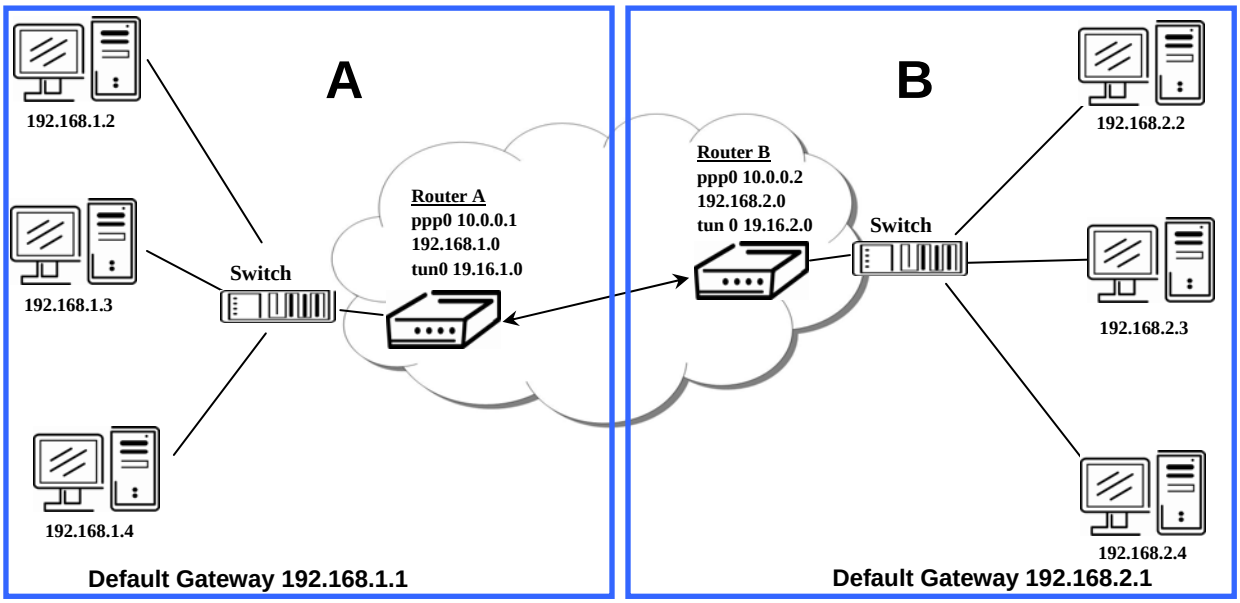


Fig. 31: Topology of example OpenVPN configuration

OpenVPN tunnel configuration:

Configuration	A	B
Protocol	UDP	UDP
UDP Port	1194	1194
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Interface IP Address	19.16.1.0	19.16.2.0
Remote Interface IP Address	19.16.2.0	19.18.1.0
Compression	LZO	LZO
Authenticate mode	none	none

Table 28: Example OpenVPN configuration

Examples of different options for configuration and authentication of OpenVPN can be found in the configuration manual OpenVPN tunnel.

1.15. *IPSec tunnel configuration*

IPsec tunnel configuration can be called up by option ***IPsec*** item in the menu. IPsec tunnel allows protected (encrypted) connection of two networks LAN to the one which looks like one homogenous. In the ***IPsec Tunnels Configuration*** window are four rows, each row for one configured one IPSec tunnel.

Item	Description
Create	This item enables the individual tunnels.
Description	This item displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Configuration IPsec tunnel.

Table 29: Overview IPsec tunnels

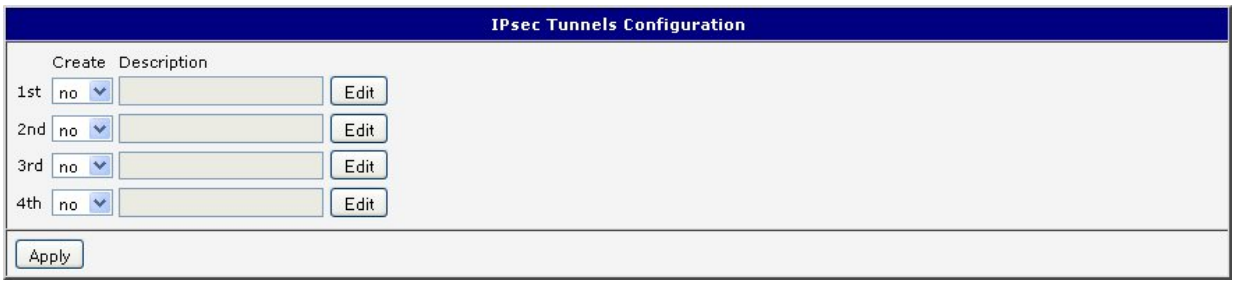


Fig. 32: IPsec tunnels configuration

Item	Description
Description	Description of tunnel.
Remote IP Address	IP address of opposite side tunnel. Can be used domain main.
Remote ID	Identification of opposite side tunnel. Parameters ID contain two parts: *hostname* and *domain-name*.
Remote Subnet	Address nets behind off - side tunnel
Remote Subnet Mask	Subnet mask behind off - side tunnel
Local ID	Identification of local side. Parameters ID contain two parts: *hostname* and *domain-name*.
Local Subnet	Local subnet address
Local subnet mask	Local subnet mask
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before connection expiry should attempt to negotiate a replacement begin. The maximum value must be less than half the parameters IKE and Key Lifetime.
Rekey Fuzz	Specifies the maximum percentage by which should be randomly increased to randomize re-keying intervals
DPD Delay	Defines time after which is made IPsec tunnel verification
DPD Timeout	By parameter *DPD Timeout* is set timeout of the answer
NAT traversal	If address translation between two end points of the IPsec tunnel is used, it needs to allow NAT Traversal
Aggressive mode	If this parameter is enabled, establishing of IPsec tunnel will be faster, but encryption will set permanently on 3DES-MD5.

Authenticate Mode	Authentication is possible to set by parameter *Authenticate mode*, at choice are following possibilities: • **Pre-shared key** - shared key for both off-side tunnel. • **X.509 Certificate** -
Pre-shared Key	sharable key for both parties tunnel
CA Certificate	This certificate is necessary to insert Authentication mode x.509.
Remote Certificate	This certificate is necessary to insert Authentication mode x.509.
Local Certificate	This certificate is necessary to insert Authentication mode x.509.
Local Private Key	This private key is necessary to insert Authentication mode x.509.
Local Passphrase	This Local Passphrase is necessary to insert Authentication mode x.509.
Extra Options	By the help of this parameter it is possible to define additional parameters of the IPsec tunnel, for example secure parameters etc.

Table 30: IPsec tunnel configuration

The certificates and private keys have to be in PEM format. As certificate it is possible to use only certificate which has start and stop tag certificate.

Random time, after which it will re-exchange of new keys are defined:

*Lifetime - (Rekey margin + random value in range (from 0 to Rekey margin * Rekey Fuzz/100))*

By default, the repeated exchange of keys held in the time range:

- Minimal time: 1h - (9m + 9m) = 42m
- Maximal time: 1h - (9m + 0m) = 51m

When setting the times for key exchange is recommended to leave the default setting in which tunnel has guaranteed security. When set higher time, tunnel has smaller operating costs and smaller the safety. Conversely, reducing the time, tunnel has higher operating costs and higher safety of the tunnel.

The changes in settings will apply after pressing the *Apply* button.

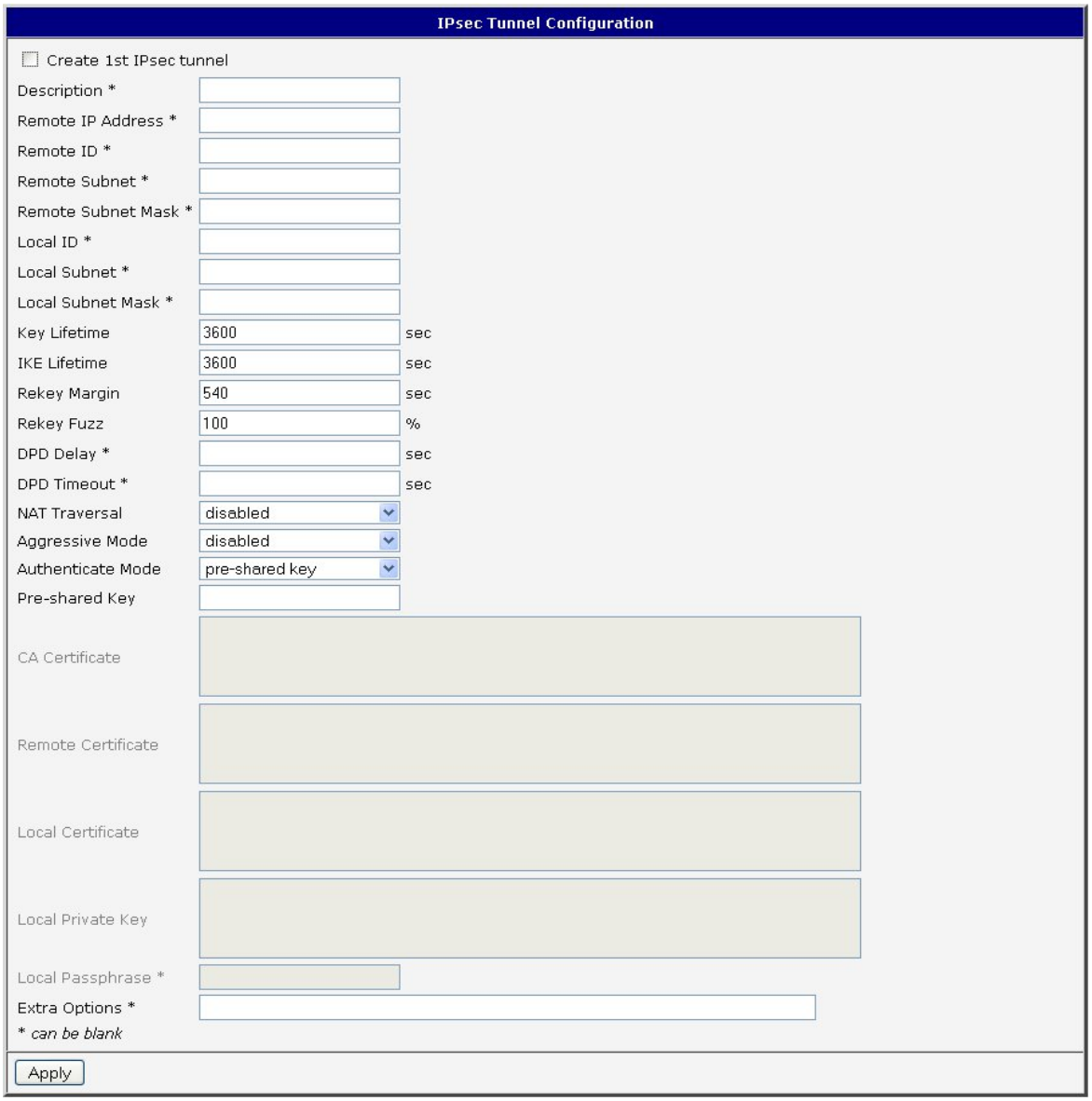


Fig. 33: IPsec tunnel configuration

Example of the IPSec Tunnel configuration:

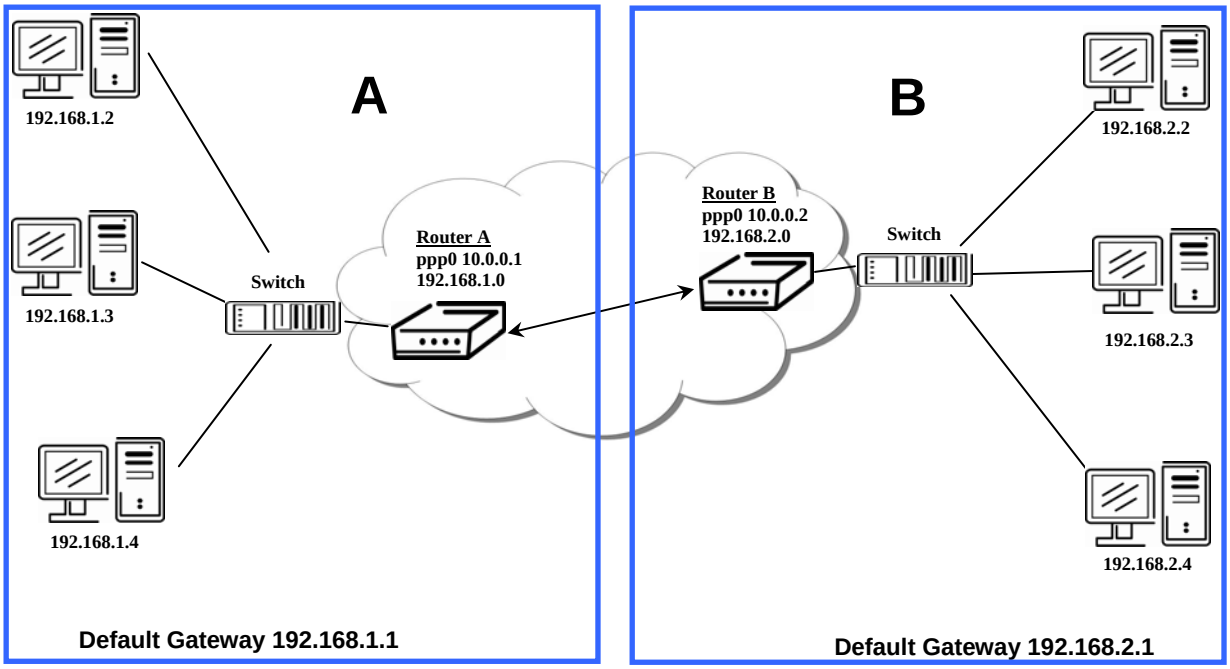


Fig. 34: Topology of example IPsec configuration

IPsec tunnel configuration:

Configuration	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Subnet	192.168.1.0	192.168.2.0
Local Subnet Mas:	255.255.255.0	255.255.255.0
Authenticate mode	pre-shared key	pre-shared key
Pre-shared key	test	test

Table 31: Example IPsec configuration

Examples of different options for configuration and authentication of IPsec can be found in the configuration manual IPsec tunnel.

1.16. *GRE tunnels configuration*

To enter the GRE tunnels configuration, select the ***GRE*** menu item. The GRE tunnel is used for connection of two networks to one that appears as one homogenous. It is possible to configure up to four GRE tunnels. In the ***GRE Tunnels Configuration*** window are four rows, each row for one configured GRE tunnel.

Item	Description
Create	This item enables the individual tunnels.
Description	This item displays the name of the tunnel specified in the configuration of the tunnel.
Edit	Configuration GRE tunnel.

Table 32: Overview GRE tunnels

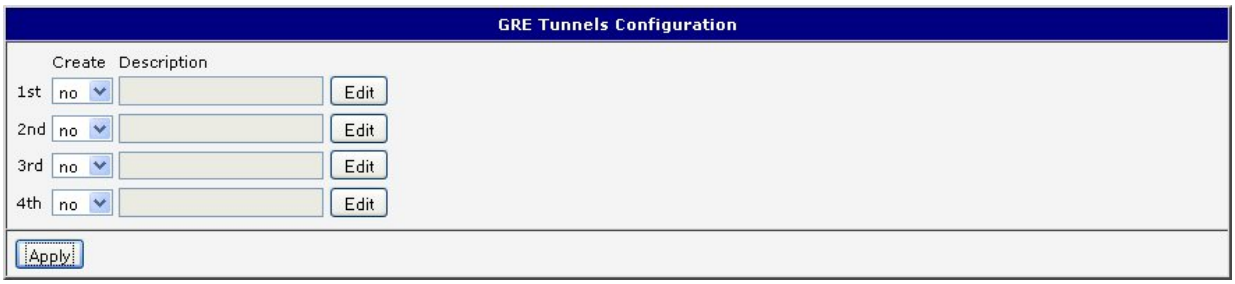


Fig. 35: GRE tunnels configuration

Item	Description
Description	Description of tunnel.
Remote IP Address	IP address of the remote side of the tunnel
Local Interface IP Address	IP address of the local side of the tunnel
Remote Interface IP Address	IP address of the remote side of the tunnel
Remote Subnet	IP address of the network behind the remote side of the tunnel
Remote Subnet Mask	Mask of the network behind the remote side of the tunnel
Pre-shared Key	An optional value that defines the 32b shared key, through which the filtered data through the tunnel. This key must be defined on both routers as same, otherwise the router will drop received packets. Using this key, the data do not provide a tunnel through.

Table 33: GRE tunnel configuration

Attention, GRE tunnel doesn't connect itself via NAT.

The changes in settings will apply after pressing the *Apply* button.

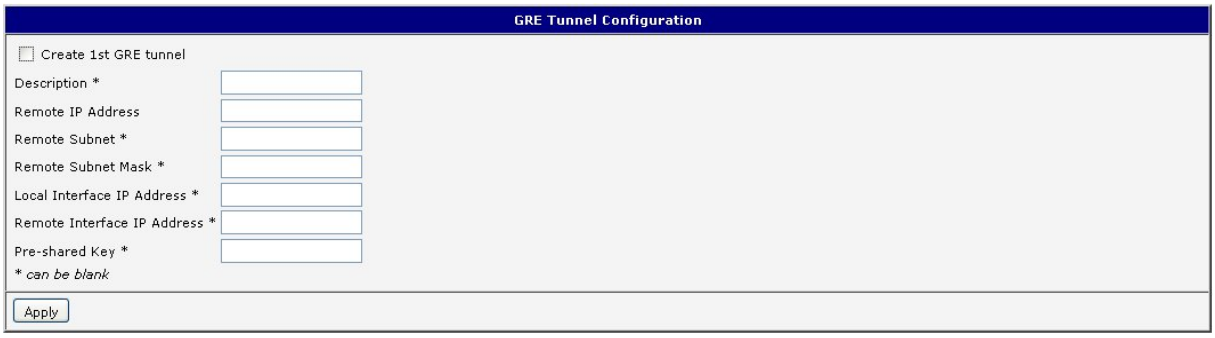


Fig. 36: GRE tunnel configuration

Example of the GRE Tunnel configuration:

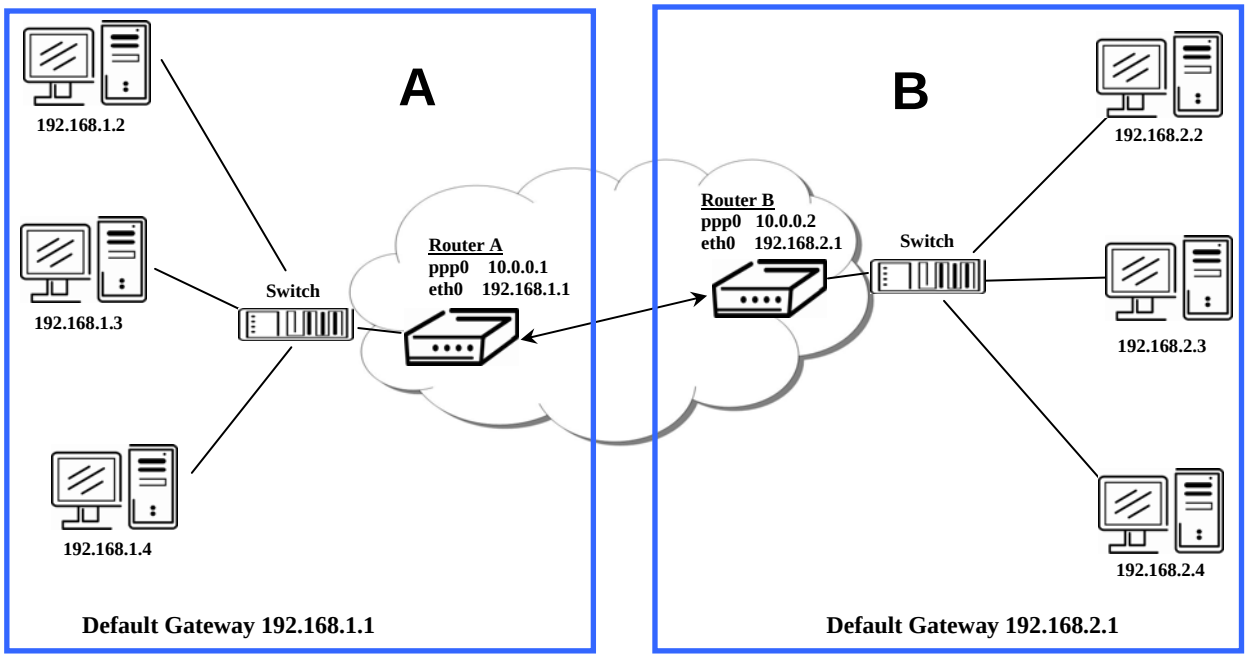


Fig. 37: Topology of GRE tunnel configuration

GRE tunnel Configuration:

Konfigurace	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

Table 34: Example GRE tunnel configuration

1.17. *L2TP tunnel configuration*

To enter the L2TP tunnels configuration, select the ***L2TP*** menu item. L2TP tunnel allows protected connection by password of two networks LAN to the one which it looks like one homogenous. The tunnels are active after selecting **Create L2TP tunnel**.

Item	Description
Mode	L2TP tunnel mode on the router side • **L2TP server -** in the case of a server must define the start and end IP address range offered by the server • **L2TP client –** in case of client must define the IP address of the server
Server IP Address	IP address of server
Client Start IP Address	Start IP address in range, which is offered by server to clients
Client End IP Address	End IP address in range, which is offered by server to clients
Local IP Address	IP address of the local side of the tunnel
Remote IP Address	IP address of the remote side of the tunnel
Remote Subnet	Address of the network behind the remote side of the tunnel
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel
Username	Username for login to L2TP tunnel
Password	Password for login to L2TP tunnel

Table 35: L2TP tunnel configuration

The changes in settings will apply after pressing the *Apply* button.

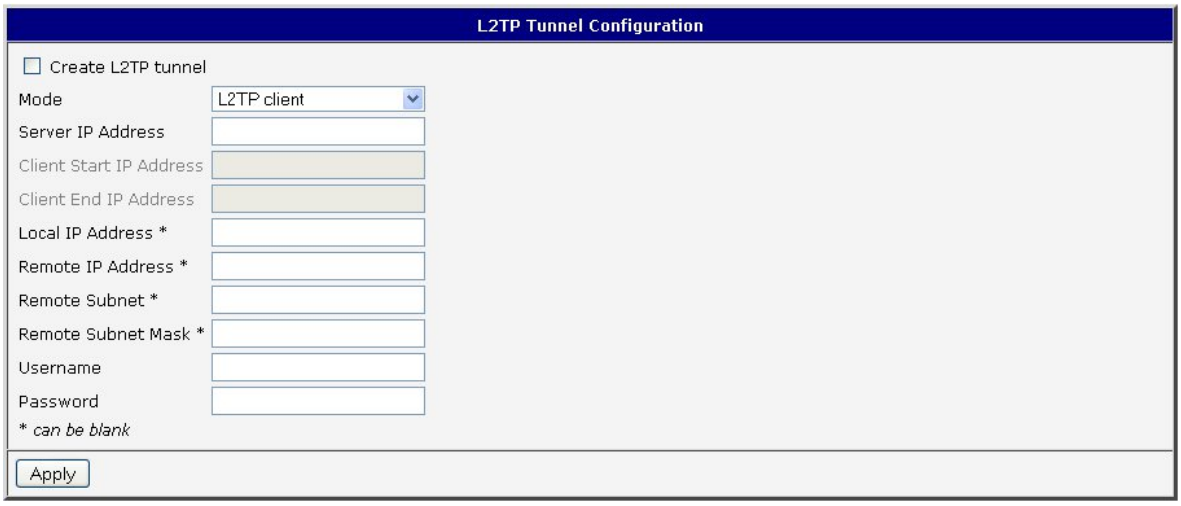


Fig. 38: L2TP tunnel configuration

Example of the L2TP Tunnel configuration:

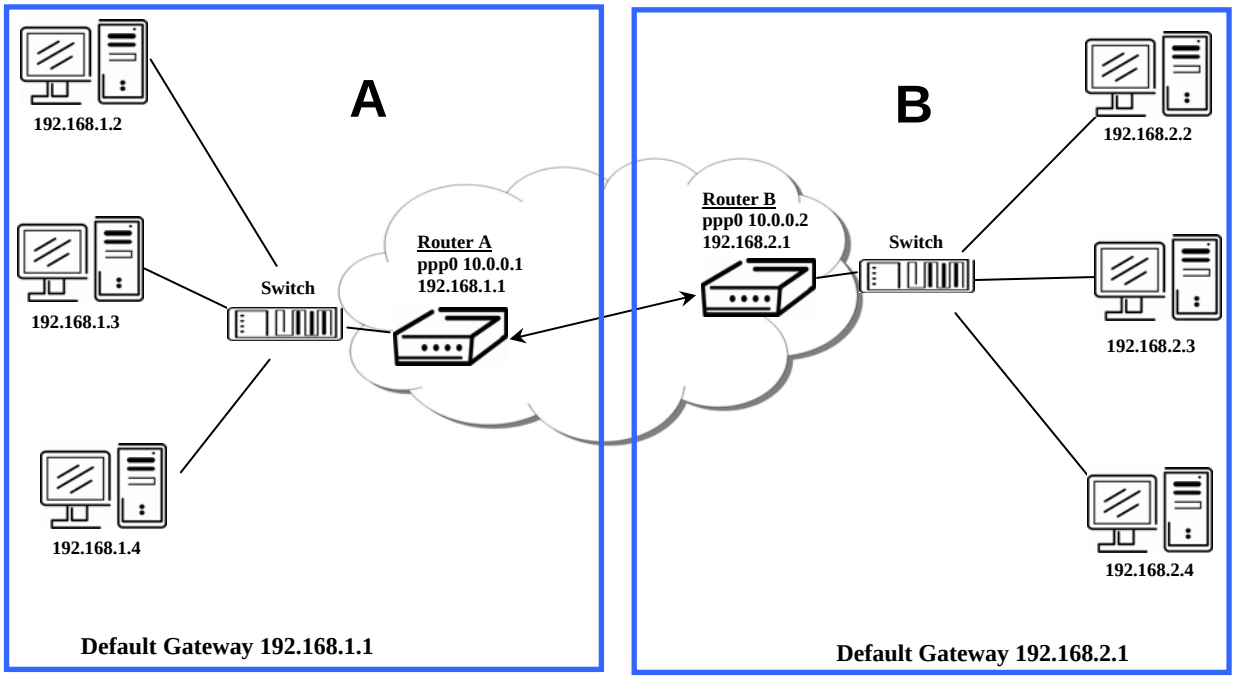


Fig. 39: Topology of example L2TP tunnel configuration

Configuration of the L2TP tunnel:

Konfigurace	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	---	10.0.0.1
Client Start IP Address	192.168.1.2	---
Client End IP Address	192.168.1.254	---
Local IP Address	192.168.1.1	---
Remote IP Address	---	---
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Table 36: Example L2TP tunel configuration

1.18. *DynDNS client configuration*

DynDNS client Configuration can be called up by option **DynDNS** item in the menu. In the window can be defined a third order domain registered on server www.dyndns.org

Item	Description
Hostname	Third order domain registered on server www.dyndns.org
Username	Username for login to DynDNS server
Password	Password for login to DynDNS server
Server	If you want to use another DynDNS service than www.dyndns.org, then enter the update server service to this item. If this item is left blank, it uses the default server members.dyndns.org.

Table 37: DynDNS configuration

Example of the DynDNS client configuration with domain conel.dyndns.org:

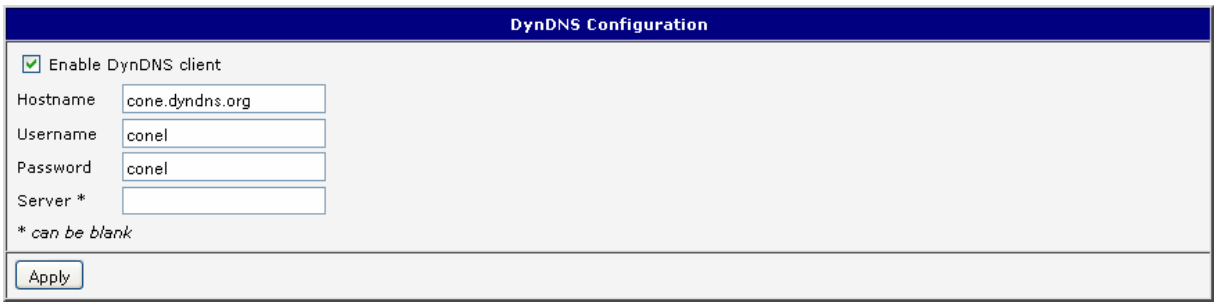


Fig. 40: Example of DynDNS configuration

1.19. *NTP client configuration*

NTP client Configuration can be called up by option **NTP** item in the menu. NTP (Network Time Protocol) allows set the exact time to the router from the servers, which provide the exact time on the network.

By parameter ***Enable local NTP service*** router is set to a mode in which it operates as an NTP server for other devices in the LAN behind the router.

By parameter ***Enable local NTP service*** it is possible to set the router in mode, that it can serve as NTP server for other devices.

Item	Description
Primary NTP Server Address	IP or domain address primary NTP server.
Secondary NTP Server Address	IP or domain address secondary NTP server.
Timezone	By this parameter it is possible to set the time zone of the router
Daylight Saving Time	By this parameter is possible to define time shift: • No - time shift is disabled • Yes - time shift is allowed

Table 38: NTP configuration

Example of the NTP configuration with set primary (ntp.cesnet.cz) and secondary (tik.cesnet.cz) NTP server and with daylight saving time:

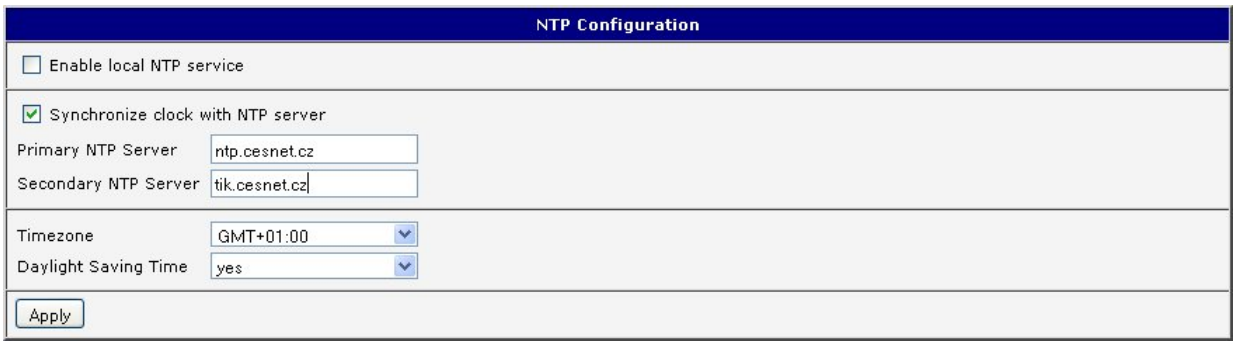


Fig. 41: Example of NTP configuration

1.20. *SNMP configuration*

To enter the **SNMP** Configuration it is possible with SNMP agent ver.1 configuration which sends information about the router, eventually about the status of the expansion port CNT or M-BUS.

SNMP (Simple Network Management Protocol) provides status information about network elements such as routers or end computers.

Item	Description
Community	Password for access to the SNMP agent.
Contact	Person who manages the router together with information how to contact this person.
Name	Designation of the router.
Location	Placing of the router.

Table 39: SNMP configuration

By choosing **Enable I/O extension** it is possible to monitor binary inputs I/O on the router.

By choosing **Enable XC-CNT extension** it is possible to monitor the expansion port CNT inputs and outputs status.

By choosing **Enable M-BUS extension** and enter the *Baudrate*, *Parity* and *Stop Bits* it is possible to monitor the meter status connected to the expansion port M-BUS status.

Item	Description
Baudrate	Communication speed.
Parity	Control parity bit: • none – Data will be sent without parity. • even – Data will be sent with even parity. • odd - Data will be sent with odd parity.
Stop Bits	Number of stop bit.

Table 40: SNMP configuration

Parameters *Enable XC-CNT extension and Enable M-BUS extension* can not be checked together.

Every monitor value is uniquely identified by the help of number identifier **OID** - *Object Identifier*. For binary input and output the following range of OID is used:

OID	Description
.1.3.6.1.4.1.30140.2.3.1.0	Binary input BIN0 (values 0,1)
.1.3.6.1.4.1.30140.2.3.2.0	Binary output OUT0 (values 0,1)

Table 41: Object identifier for binary input and output

For the expansion port CNT the following range of OID is used:

OID	Description
.1.3.6.1.4.1.30140.2.1.1.0	Analogy input AN1 (range 0-4095)
.1.3.6.1.4.1.30140.2.1.2.0	Analogy input AN2 (range 0-4095)
.1.3.6.1.4.1.30140.2.1.3.0	Counter input CNT1 (range 0-4294967295)
.1.3.6.1.4.1.30140.2.1.4.0	Counter input CNT2 (range 0-4294967295)
.1.3.6.1.4.1.30140.2.1.5.0	Binary input BIN1 (values 0,1)
.1.3.6.1.4.1.30140.2.1.6.0	Binary input BIN2 (values 0,1)
.1.3.6.1.4.1.30140.2.1.7.0	Binary input BIN3 (values 0,1)
.1.3.6.1.4.1.30140.2.1.8.0	Binary input BIN4 (values 0,1)
.1.3.6.1.4.1.30140.2.1.9.0	Binary output OUT1 (values 0,1)

Table 42: Object identifier for CNT port

For the expansion port M-BUS the following range of OID is used:

OID	Description
.1.3.6.1.4.1.30140.2.2.<address>.1.0	IdNumber – meter number
.1.3.6.1.4.1.30140.2.2.<address>.2.0	Manufacturer
.1.3.6.1.4.1.30140.2.2.<address>.3.0	Version – specified meter version
.1.3.6.1.4.1.30140.2.2.<address>.4.0	Medium – type of metered medium
.1.3.6.1.4.1.30140.2.2.<address>.5.0	Status – errors report
.1.3.6.1.4.1.30140.2.2.<address>.6.0	0. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.7.0	0. measured value
.1.3.6.1.4.1.30140.2.2.<address>.8.0	1. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.9.0	1. measured value
…	
.1.3.6.1.4.1.30140.2.2.<address>.100.0	47. VIF – value information field
.1.3.6.1.4.1.30140.2.2.<address>.101.0	47. measured value

Table 43: Object identifier for M-BUS port

The meter address can be from range 0..254 when 254 is broadcast.

Example of SNMP settings and readout:

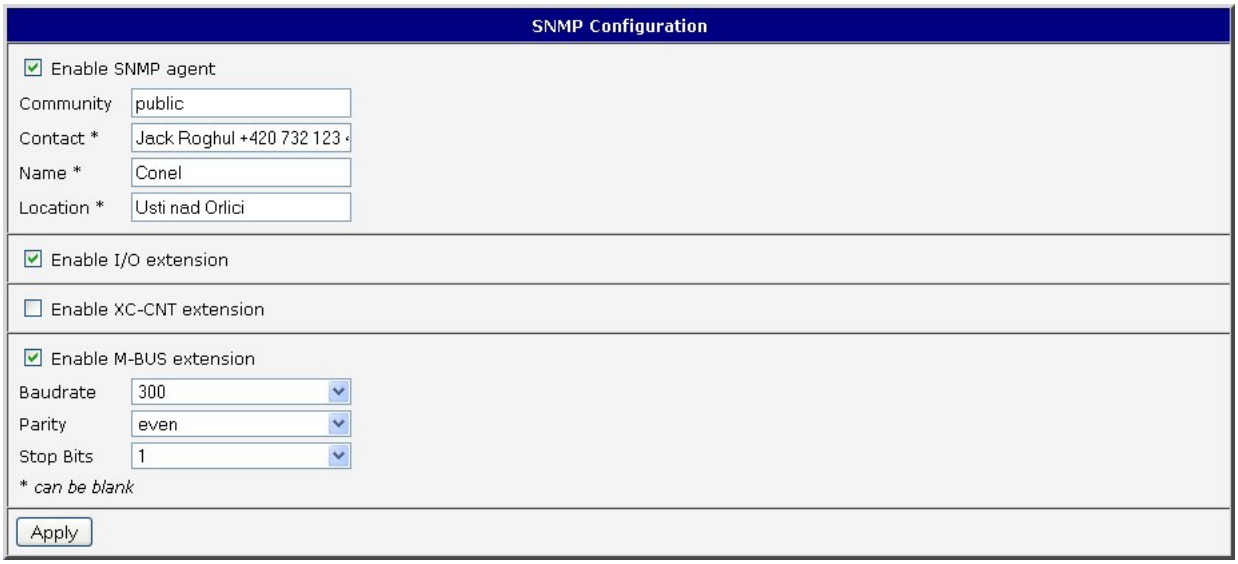


Fig. 42: Example of SNMP configuration

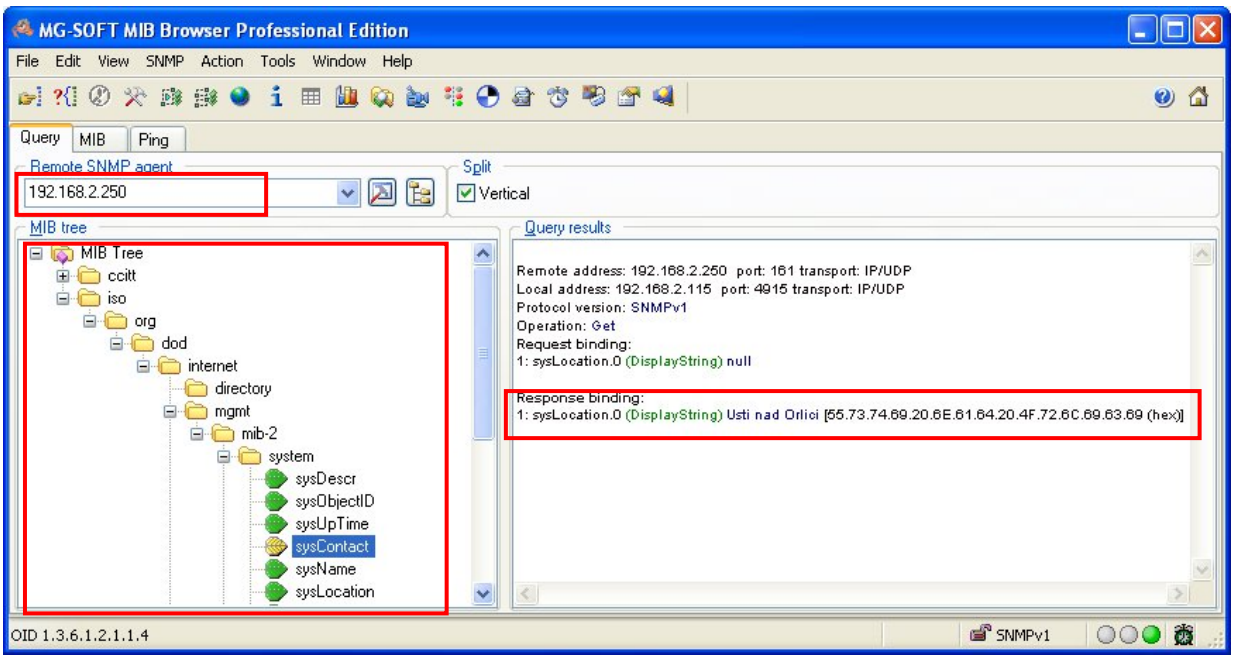


Fig. 43: Example of the MIB browser

It is important to set the IP address of the SNMP agent (router) in field *Remote SNMP agent*. After enter the IP address is in a *MIB tree* part is possible show object identifier.

The path to objects is:

iso->org->dod->internet->private->enterprises->conel->protocols.

The path to information about router is:

iso->org->dod->internet->mgmt->mib-2->system

1.21. *SMTP configuration*

To enter the **SMTP** it is possible configure SMTP (Simple Mail Transfer Protocol) client, which is set by sending emails.

Item	Description
SMTP Server Address	IP or domain address of the mail server.
Username	Name to email account.
Password	Password to email account.
Own Email Address	Address of the sender.

Fig. 44: SMTP client configuration

Mobile operator can block other SMTP servers, then you can use only the SMTP server of operator.

Example settings SMTP client:

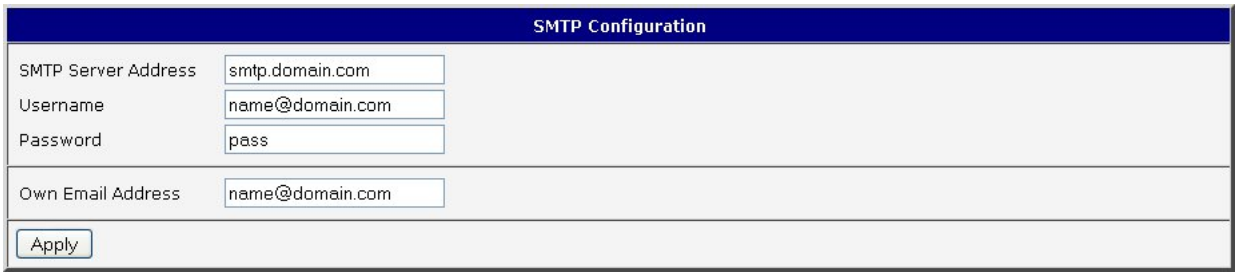


Fig. 45: SMTP configuration

E-mail can be send from the Startup script. This command is used to email with following parameters.

- -t receiver Email address
- -s subject
- -m message
- -a appendix
- -r number of attempts to send email (default set 2 attempts)

Commands and parameters can be entered only in lowercase.

Example to send email:

email –t name@domain.com –s "subject" –m "message" –a c:\directory\abc.doc –r 5

This command sends e-mail to address *jack@google.com* with the subject "*subject*", body message "message" and annex "abc.doc" right from the directory c:\directory\ and 5 attempts to send.

1.22. *SMS configuration*

The industrial router XR5i v2 is not availability item SMS Configuration.

SMS Configuration can be called up by option **SMS** item in the menu. SMS configuration defines the options for sending SMS messages from the router at different defined events and states of the router. In the first part of window it configuration send SMS.

Item	Description
Send SMS on power up	Automatic sending of SMS messages after power up
Send SMS on PPP connect	Automatic sending SMS message after PPP connection.
Send SMS on PPP disconnect	Automatic sending SMS message after PPP disconnection.
Send SMS when datalimit exceeded	Automatic sending SMS message after datalimit exceeded.
Send SMS when binary input on I/O port (BIN0) is active	Automatic sending SMS message after binary input on I/O port (BIN0) is active. Text of message is intended parameter BIN0.
Send SMS when binary input on expansion port (BIN1-BIN4) is active	Automatic sending SMS message after binary input on expansion port (BIN1-BIN4) is active. Text of message is intended parameter BIN1 - BIN4.
Phone Number 1	Telephone numbers for sending automatically generated SMS.
Phone Number 2	
Phone Number 3	
Unit ID	The name of the router that will be sent in an SMS.
BIN0 - SMS	SMS text messages when activate the binary input on the router.
BIN1 - SMS	SMS text messages when activate the binary input on the expansion port.
BIN2 - SMS	SMS text messages when activate the binary input on the router.
BIN3 - SMS	SMS text messages when activate the binary input on the router.
BIN4 - SMS	SMS text messages when activate the binary input on the router.

Table 44: Send SMS configuration

In the second part of the window it is possible to set function **Enable remote control via SMS**. After this it is possible to establish and close PPP connection by SMS message.

Item	Description
Phone Number 1	This control can be configured for up to three numbers. If is set *Enable remote control via SMS,* all incoming SMS are processed and deleted. In the default settings this parameter is turned on.
Phone Number 2	
Phone Number 3	

Table 45: Control via SMS configuration

If no phone number is filled in, then it is possible to restart the router with the help of SMS in the form of Reboot from any phone number. While filling of one, two or three numbers it is possible to control the router with the help of an SMS sent only from these numbers. While filling of sign “*” it is possible control the router with the help of an SMS sent from every numbers.

Control SMS message doesn’t change the router configuration. If the router is switched to offline mode by the SMS message the router will be in this mode up to next restart. This behavior is the same for all control SMS messages.

It is possible to send controls SMS in the form:

SMS	Description
go online sim 1	Switch to SIM1 card
go online sim 2	Switch to SIM2 card
go online	Switch router in online mode
go offline	PPP connection termination
set out0=0	Set output I/O connector on 0
set out0=1	Set output I/O connector on 1
set out1=0	Set output expansion port XC-CNT on 0
set out1=1	Set output expansion port XC-CNT on 1
set profile std	Set standard profile
set profile alt1	Set alternative profile 1
set profile alt2	Set alternative profile 2
set profile alt3	Set alternative profile 3
reboot	Router reboot
get ip	Router send answer with IP address SIM card

Table 46: Control SMS

By choosing ***Enable AT-SMS protocol on expansion port 1*** and *Baudrate* it is possible to send/receive an SMS on the serial Port 1.

Item	Description
Baudrate	Communication speed expansion port 1

Table 47: Send SMS on serial PORT1 configuration

By choosing ***Enable AT-SMS protocol on expansion port 2*** and *Baudrate* it is possible to send/receive an SMS on the serial Port 2.

Item	Description
Baudrate	Communication speed expansion port 1

Table 48: Send SMS on serial PORT1 configuration

By choosing ***Enable AT-SMS protocol on TCP port*** and enter the *TCP port* it is possible to send/receive an SMS on the TCP port. SMS messages are sent by the help of a standard AT commands.

Item	Description
TCP Port	TCP port on which will be allowed to send/receive SMS messages.

Table 49: Send SMS on ethernet PORT1 configuration

1.22.1. Send SMS

The SMS is possible to do for example in HyperTerminal program. After establishing connection with the router via serial interface or Ethernet, it is possible to do with SMS by the help of the next AT commands.

AT commands	Description
AT+CMGF=1	Set the text mode for SMS writing
AT+CMGS=”tel. number”	Commands enables to send SMS on entered tel. number
AT+CMGL=ALL	List of all SMS messages
AT+CMGR=<index>	Read of the definite SMS (all SMS has our index)
AT+CMGD=<index>	SMS delete according to index

Table 50: AT commands for work with SMS

For the text mode for SMS writing is used command *AT+CMGF=1*.

AT+CMGF=1 Enter

OK

The SMS message is created by the help of command *AT+CMGS=<tel. number>*. After *Enter* button is pressed is displayed mark >, behind this mark it is possible to write your own SMS message. The SMS message is sent by the help of *CTRL+Z* (SMS sending takes a few minutes). SMS writing is possible to cancel by pressing *Esc*.

AT+CMGS="712123456" Enter

>***Hello World!*** CTRL+Z (keys combination)

OK

It is possible to find the new SMS by the help of command *AT+CMGL=ALL*. This command reproaches all SMS messages.

AT+CMGL="ALL" Enter

+CMGL: <index>, <status>,<sender number>, ,<date>,<time>
SMS text.

+CMGL: 1,"REC UNREAD","+420721123456", ,"08/02/02, 10:33:26+04"
Hello World!
where <index> is ordinal number of the SMS,

<status> is SMS status:

REC UNREAD – SMS unread
REC READ – SMS read
STO UNSENT – stored unsent SMS
STO SENT – stored sent SMS
ALL – all SMS messages

<sender number> is tel. number from which the SMS was receive,

<date> is date of SMS received,

<time> is time of SMS received.

It is possible to read the new SMS message by command AT+CMGR=<index>.

AT+CMGR=1 Enter

+CMGL: <index>, <status>,<sender number>, ,<date>,<time>
SMS text.

+CMGL: 1,"REC READ","+420721123456", ,"08/01/12, 9:48:04+04"
Hello World!

Received SMS is possible to delete by command AT+CMGD=<index>.

AT+CMGD=1 Enter

OK

After powering up the router, at introduction of the telephone number comes SMS in the form of:

Router (Unit ID) has been powered up.GSM signal strength –xx dBm.

After PPP connect, at introduction of the telephone number comes SMS in the form:

Router (Unit ID) has established PPP connection. IP address xxx.xxx.xxx.xxx

After PPP disconnect, at introduction of the telephone number comes SMS in the form:

Router (Unit ID) has lost PPP connection. IP address xxx.xxx.xxx.xxx

Configuration of sending this SMS is following:

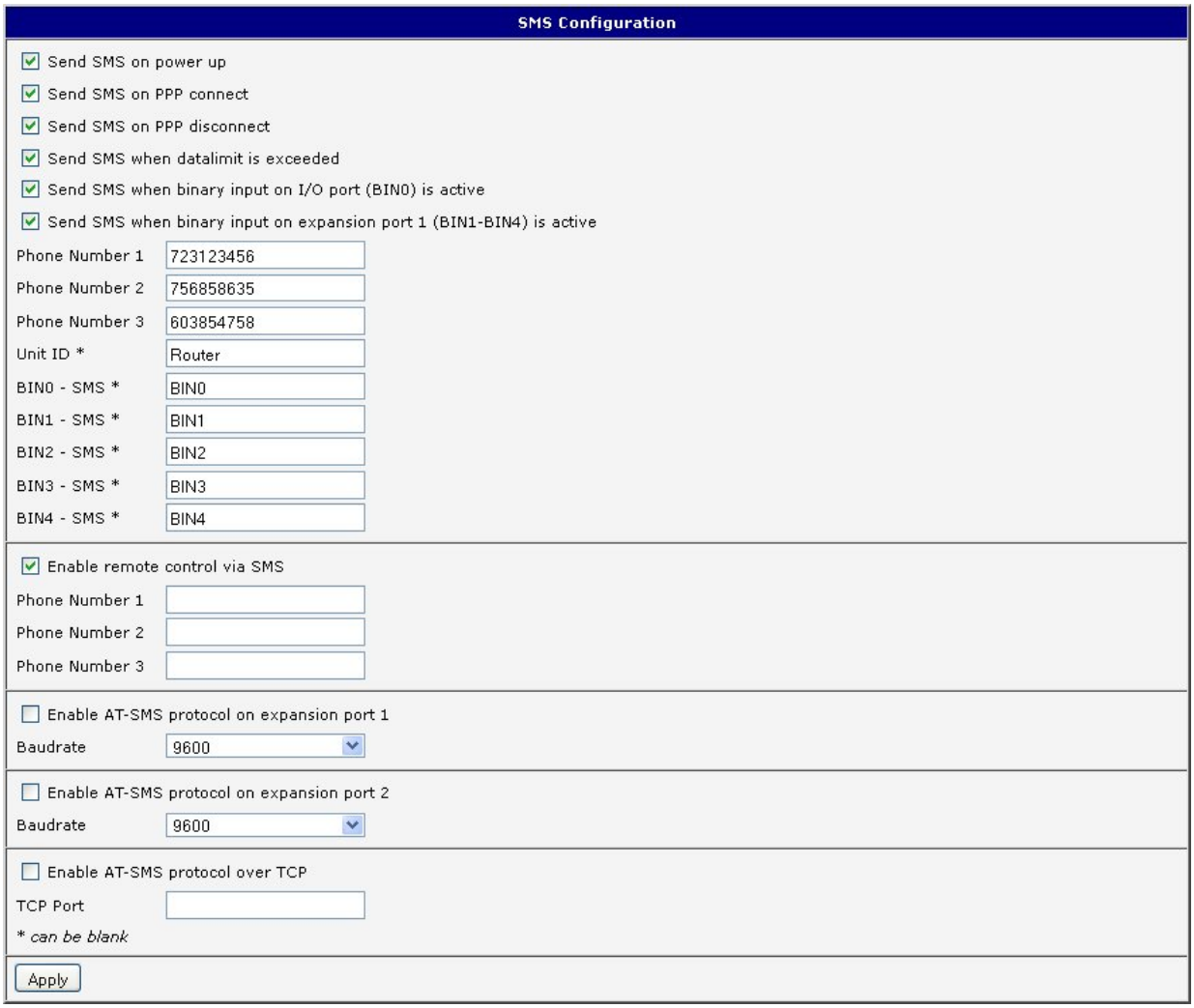


Fig. 46: Example of SMS configuration 1

Example of the router configuration for SMS sending via serial interface on the PORT1:

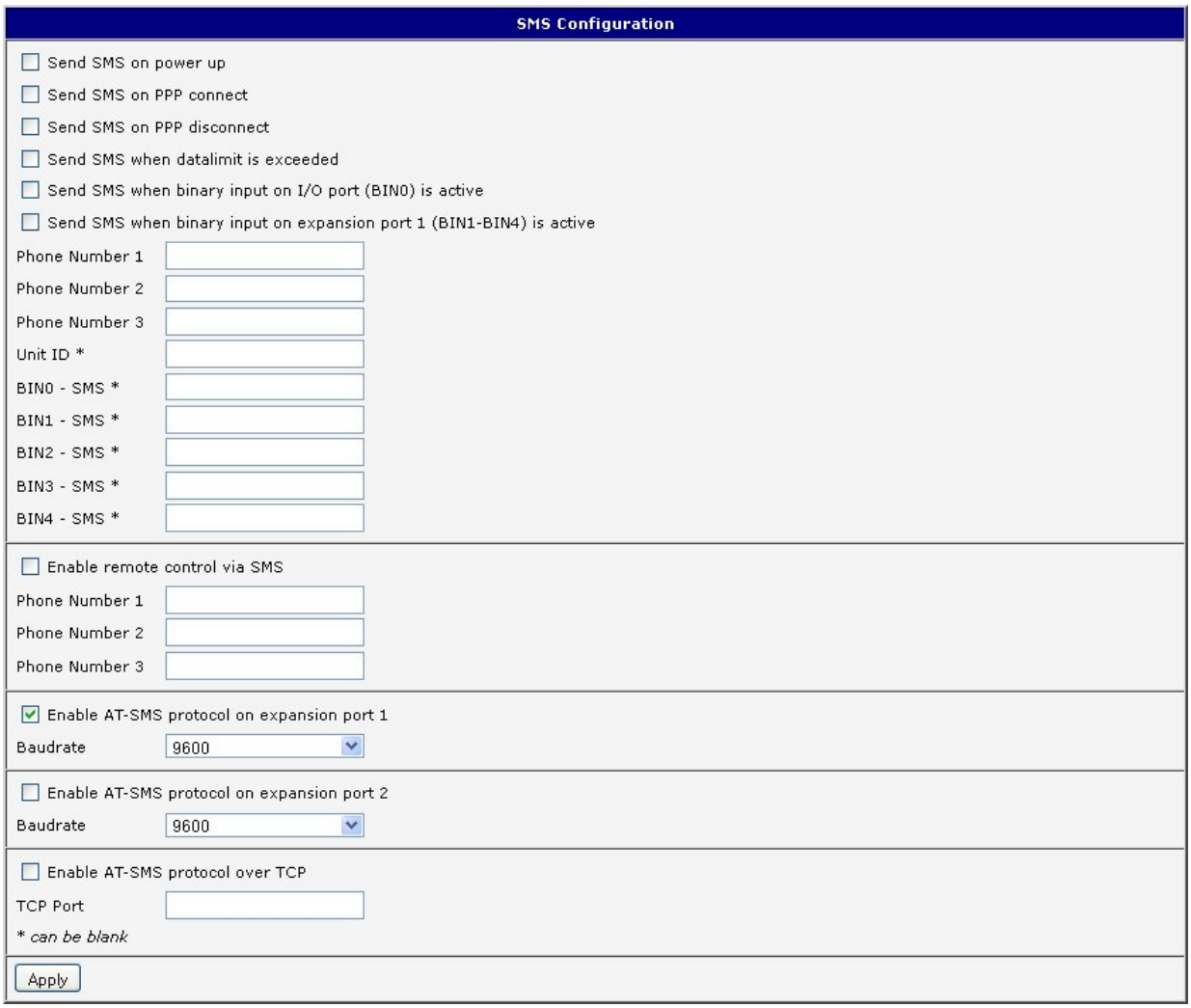


Fig. 47: Example of SMS configuration 2

Example of the router configuration for controlling via SMS from every phone numbers:

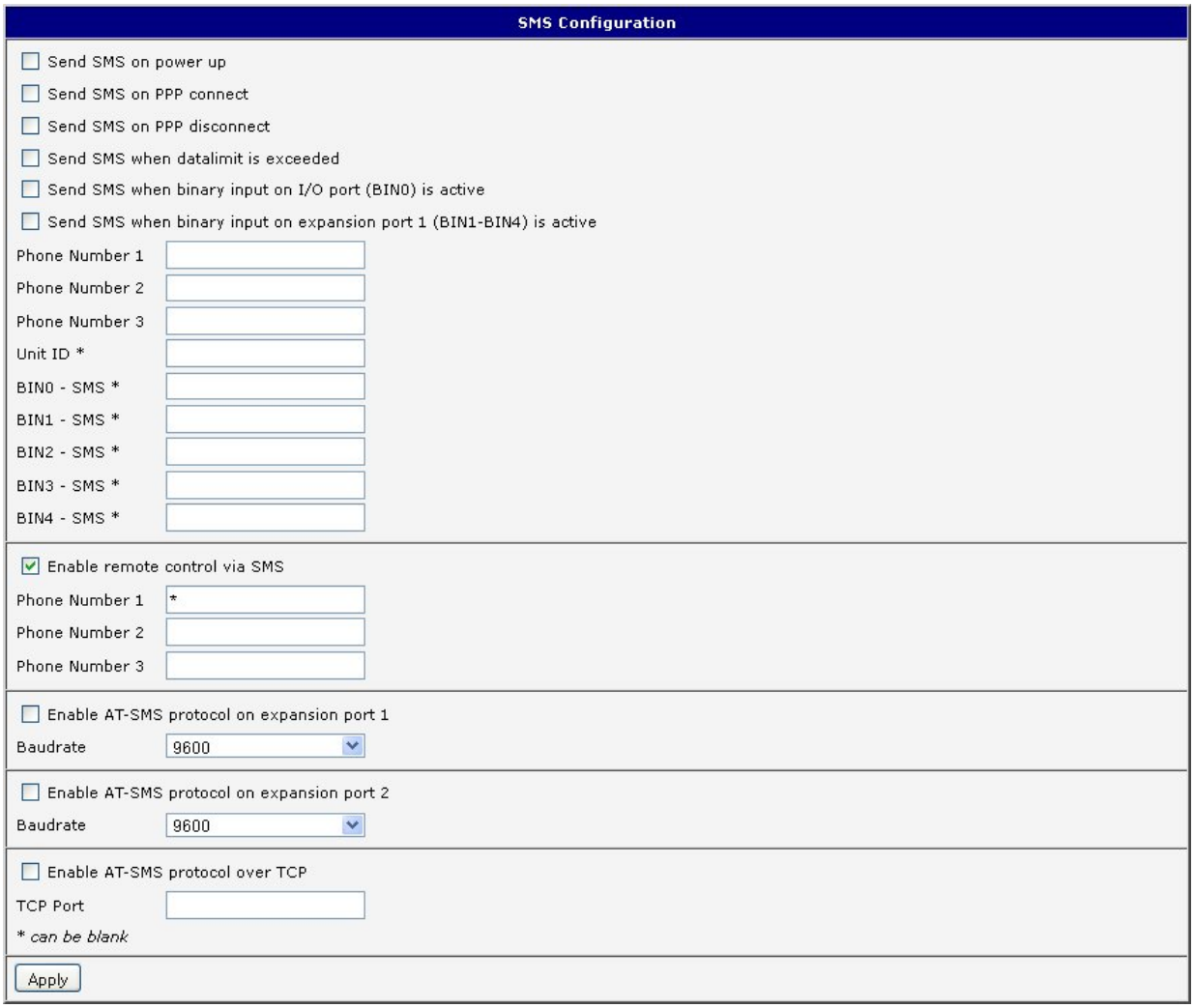


Fig. 48: Example of SMS configuration 3

Example of the router configuration for controlling via SMS from two phone numbers:

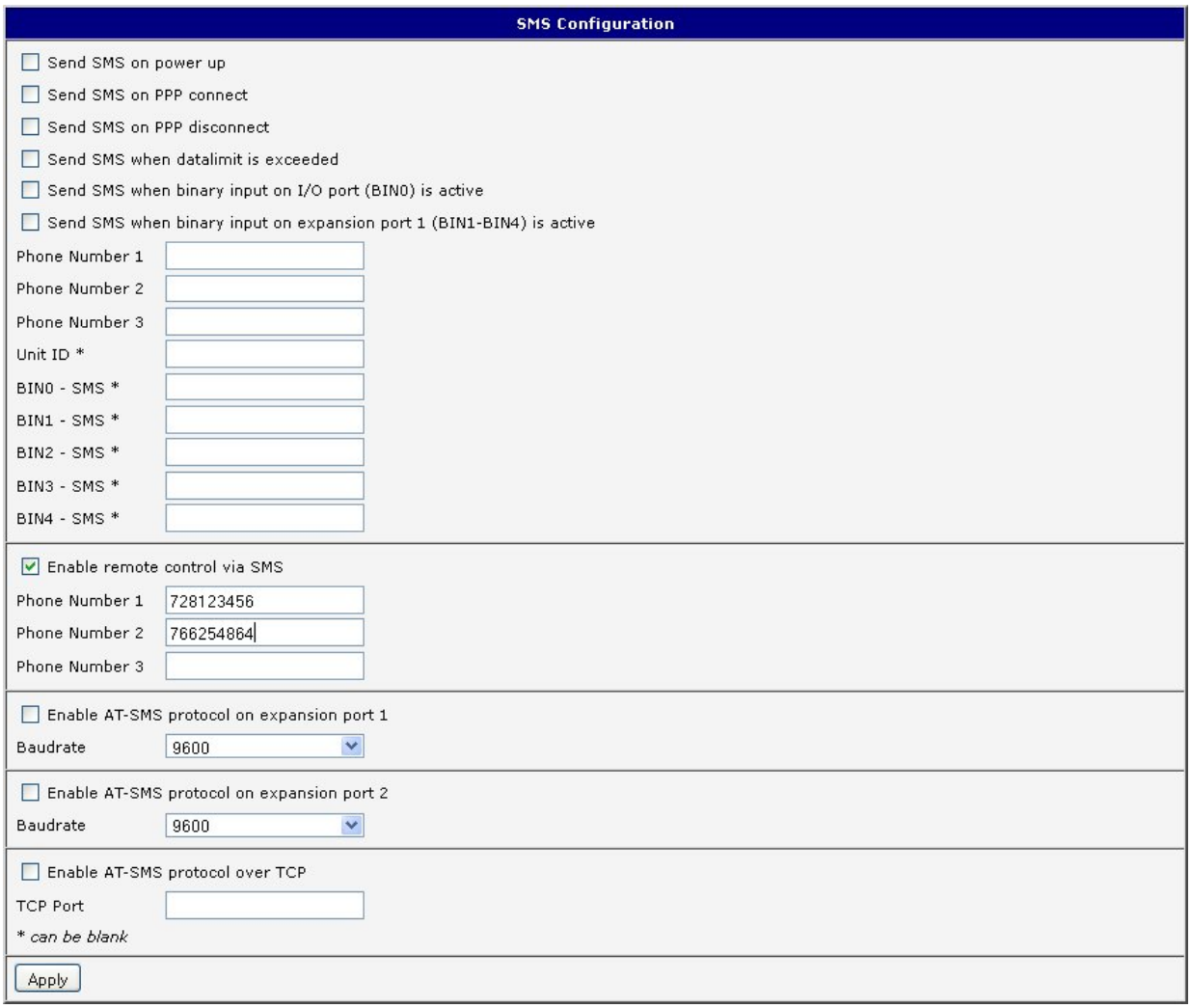


Fig. 49: Example of SMS configuration 4

1.23. *Expansion port configuration*

Configuring of the expansion ports PORT1 and PORT2 can cause selecting **Expansion Port 1** or **Expansion Port 2**.

Item	Description
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit • none - Will be sent without parity. • even - Will be sent with even parity. • odd - Will be sent with odd parity.
Stop Bits	Number of stop bit.
Split Timeout	Time to rupture reports. If you receive will identify the gap between two characters, which is longer than the parameter value in milliseconds. Then all of the received data compiled and sent the message.
Protocol	Protocol: • TCP - communication using a linked protocol TCP • UDP - communication using a unlinked protocol UDP
Mode	Mode of connection: • TCP server - The router will listen to incoming requests about TCP connection. • TCP client - The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	In mode *TCP client* it is necessary to enter the *Server address* and final *TCP port*.
TCP Port	In both modes of connection is necessary to specify the TCP port on which the router will communicate TCP connections.

Table 51: Expansion PORT configuration 1

After check ***Check TCP connection,*** it activates established of TCP connection.

Item	Description
Keepalive Time	Time, after which it will carry out verification of the connection
Keepalive Interval	Waiting time on answer
Keepalive Probes	Number of tests

Table 52: Expansion PORT configuration 2

When you select items **Use CD as indicator of the TCP connection** is activated function indication TCP connection using signal CD (DTR on the router).

CD	Description
Active	TCP connection is on
Nonactive	TCP connection is off

Table 53: CD signal description

When you select items **Use DTR as control of TCP connection** is activated function control TCP connection using signal DTR (CD on the router).

DTR	Description server	Description client
Active	The router allows establishing a TCP connection.	Router starts TCP connection.
Nonactive	The router does not permit establishing a TCP connection.	Router stops TCP connection.

Table 54: DTR signal description

The changes in settings will apply after pressing the *Apply* button.

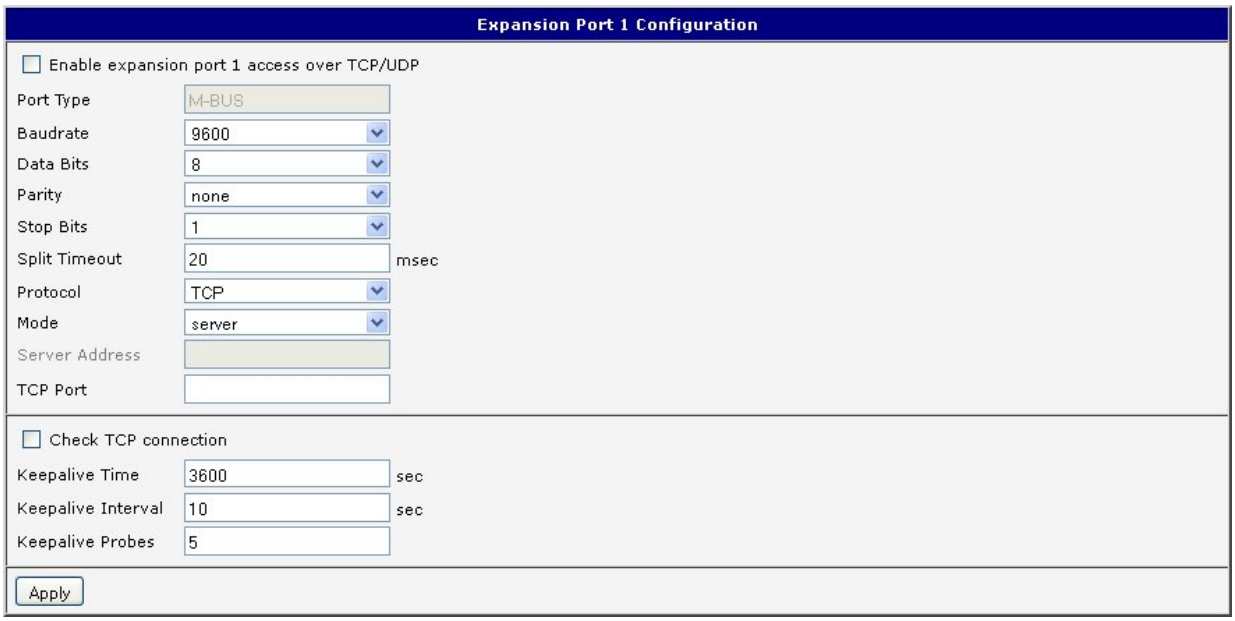


Fig. 50: Expansion port configuration

Example of external port configuration:

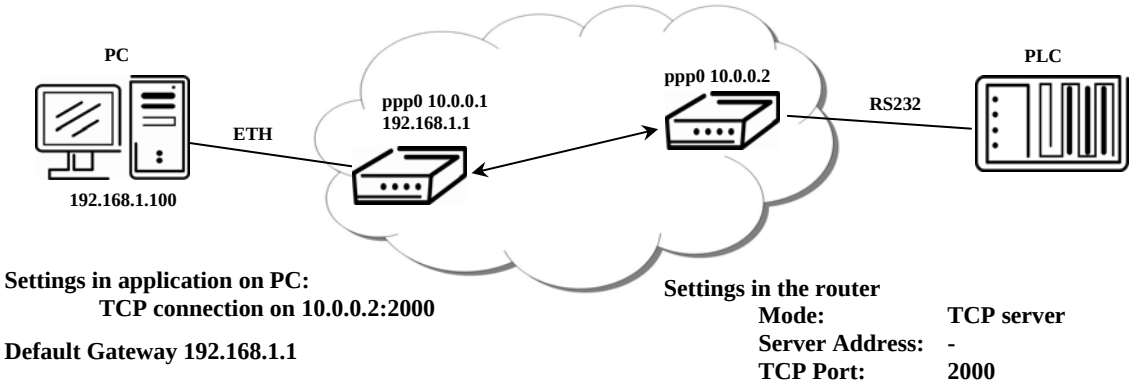


Fig. 51: Example of expansion port configuration 1

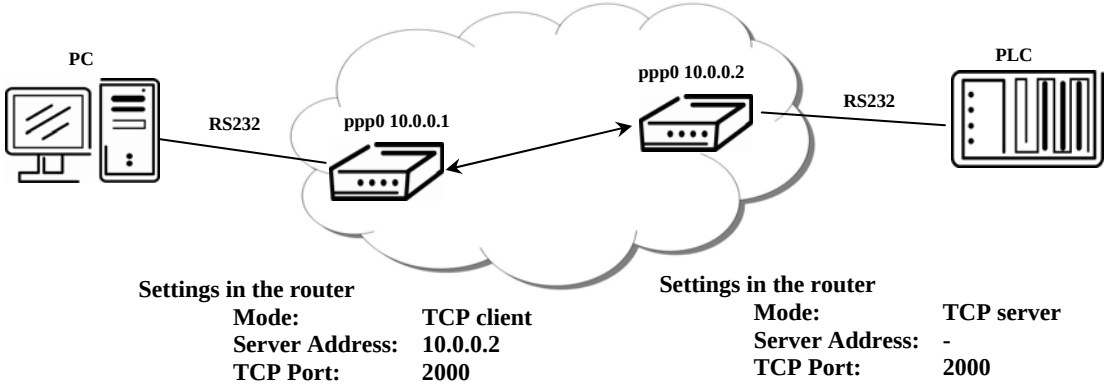


Fig. 52: Example of expansion port configuration 2

1.24. *USB port configuration*

The USB port configuration can be called up by airbrush option ***USB Port*** in menu. Configuration can be done, if we have USB/RS232 converter.

Item	Description
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit • none - Will be sent without parity. • even - Will be sent with even parity. • odd - Will be sent with odd parity.
Stop Bits	Number of stop bit.
Split Timeout	Time to rupture reports. If you receive will identify the gap between two characters, which is longer than the parameter value in milliseconds. Then all of the received data compiled and sent the message.
Protocol	Communication protocol: • TCP - communication using a linked protocol TCP • UDP - communication using a unlinked protocol UDP
Mode	Mode of connection: • TCP server - The router will listen to incoming requests about TCP connection. • TCP client - The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	In mode *TCP client* it is necessary to enter the *Server address* and final *TCP port*.
TCP Port	In both modes of connection is necessary to specify the TCP port on which the router will communicate TCP connections.

Table 55: USB port configuration 1

After check ***Check TCP connection,*** it activates verification of established TCP connection.

Item	Description
Keepalive Time	Time, after which it will carry out verification of the connection
Keepalive Interval	Waiting time on answer
Keepalive Probes	Number of tests

Table 56: USB PORT configuration 2

When you select items **Use CD as indicator of the TCP connection** is activated function indication TCP connection using signal CD (DTR on the router).

CD	Description
Active	TCP connection is on
Nonactive	TCP connection is off

Table 57: CD signal description

When you select items **Use DTR as control of TCP connection** is activated function control TCP connection using signal DTR (CD on the router).

DTR	Description server	Description client
Active	The router allows establishing a TCP connection.	Router starts TCP connection.
Nonactive	The router does not permit establishing a TCP connection.	Router stops TCP connection.

Table 58: DTR signal description

Supported USB/RS232 converters:

- FTDI
- Prolific PL2303
- Silicon Laboratories CP210× (Podporován od firmware verze 3.0.1)

The changes in settings will apply after pressing the *Apply* button

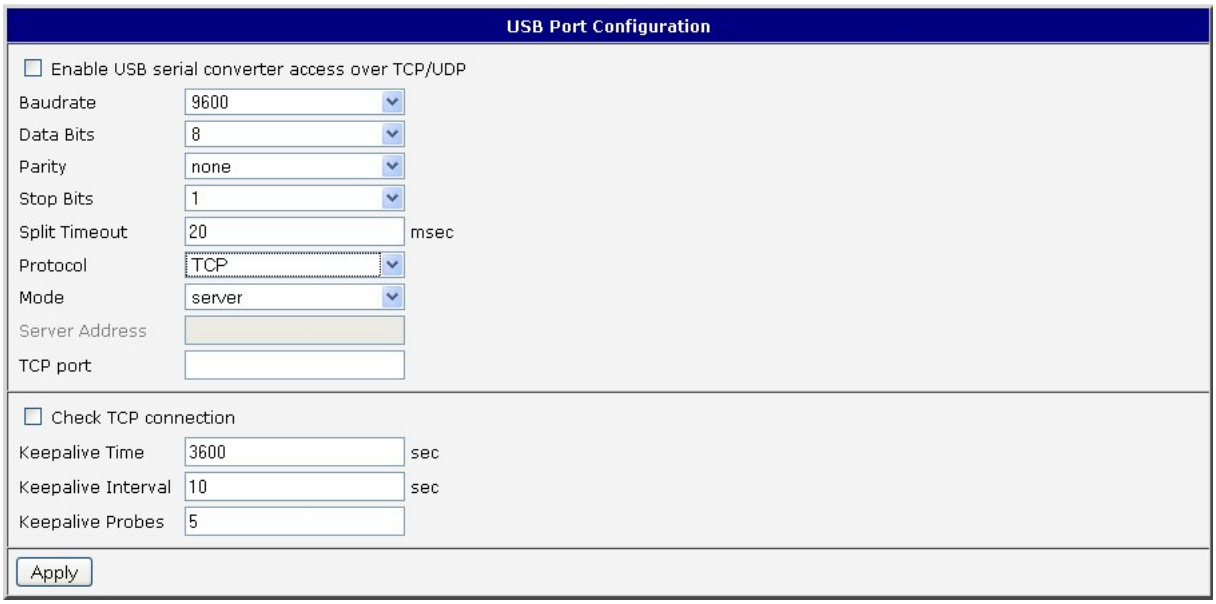


Fig. 53: USB configuration

Example of USB port configuration:

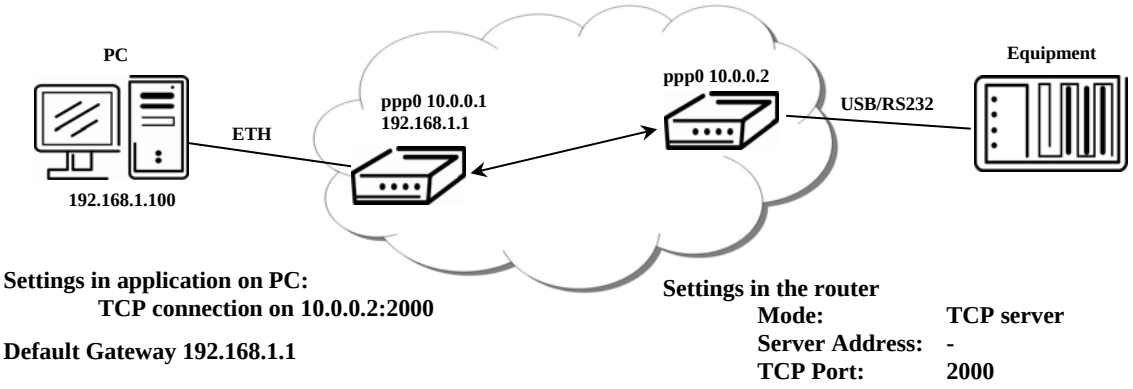


Fig. 54: Example of USB port configuration 1

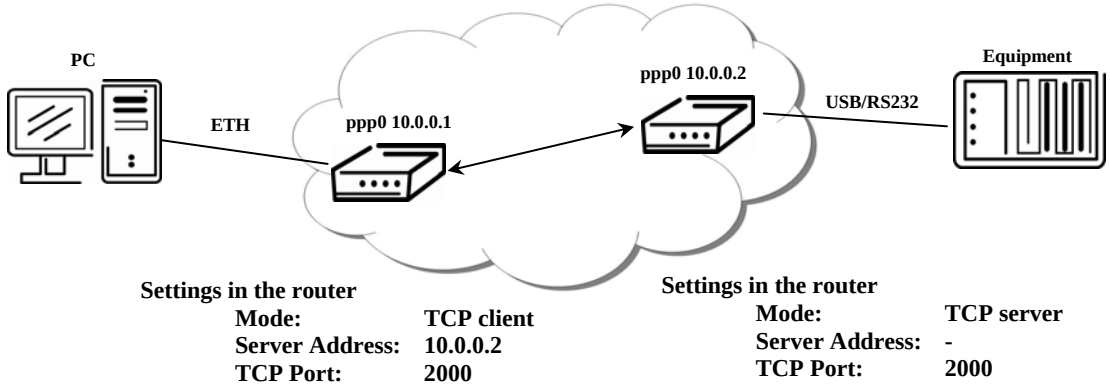


Fig. 55: Example of USB port configuration 2

1.25. *Startup script*

In the window ***Startup Script*** it is possible to create own scripts which will be executed after all initial scripts.

The changes in settings will apply after pressing the *Apply* button.

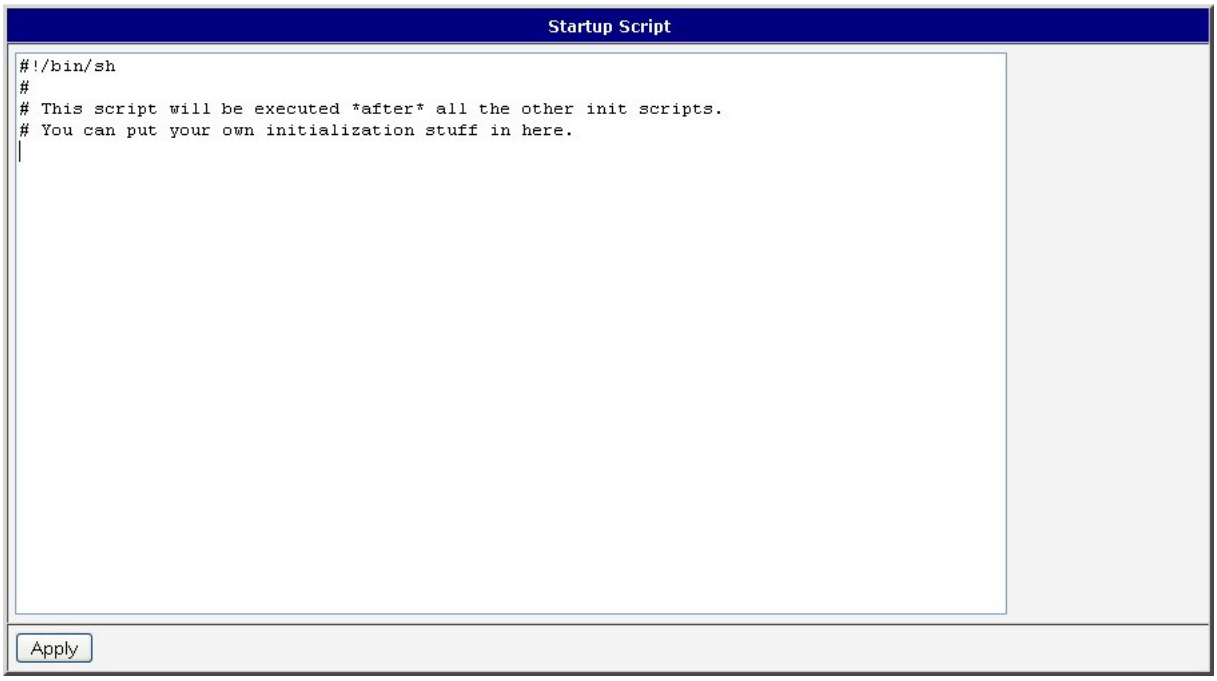


Fig. 56: Startup script

Change take effect after shut down and witch on router by the help of button *Reboot* in web administration or by SMS message.

Example of Startup script: When start the router, stop syslogd program and start syslogd with remote logging on address 192.168.2.115 and limited to 100 entries listing.

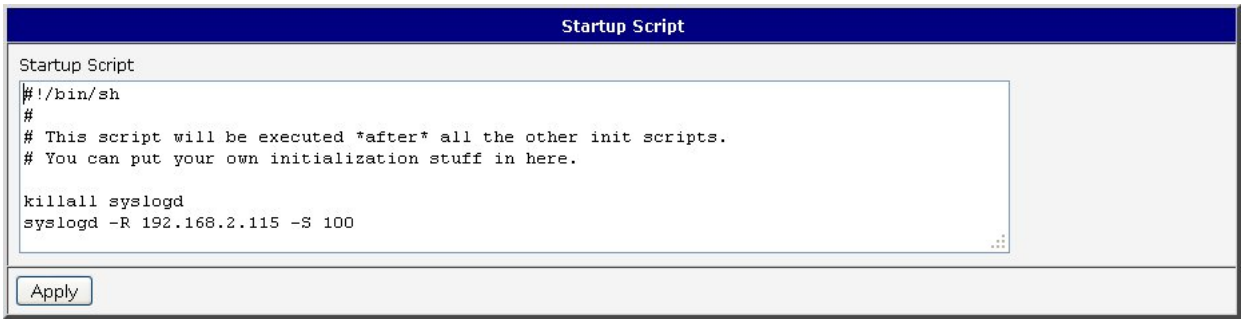


Fig. 57: Example of Startup script

1.26. *Up/Down script*

In the window **Up/Down Script** it is possible to create own scripts. In the item **Up script** is defined scripts, which begins after establishing a PPP/WAN connection. In the item **Down Script** is defines script, which begins after lost a PPP/WAN connection.

The changes in settings will apply after pressing the *Apply* button.

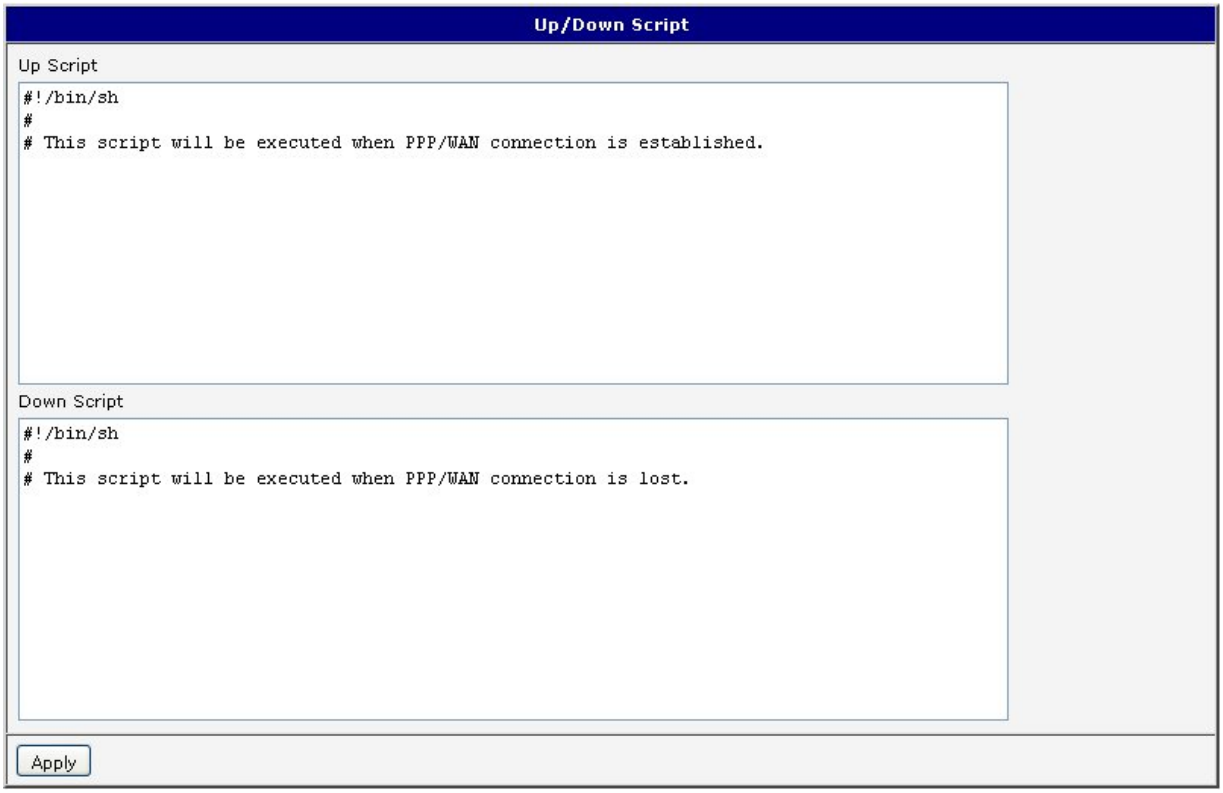


Fig. 58: Up/Down script

Example of UP/Down script: After establishing or lost a PPP connection, the router sends an email with information about establishing or loss a PPP connection.

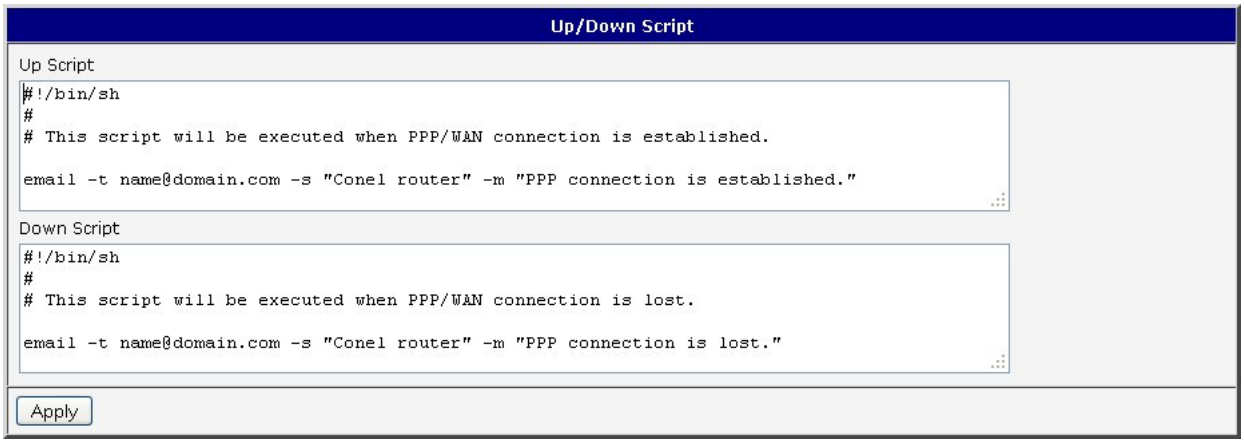


Fig. 59: Example of Up/Down script

1.27. *Automatic update configuration*

In the window **Automatic update** it is possible to set automatic configuration update. This choice enables that the router automatically downloads the configuration and the newest firmware from the server itself. The configuration and firmware are stores on the server.

By ***Enable automatic update of configuration*** it is possible to enable automatic configuration update and by ***Enable automatic update of firmware*** it is possible to enable firmware update.

Item	Description
Source	In the item source can be set, where new firmware download: • ***HTTP/FTP server*** - new firmware or configuration look at address in the Base URL item • ***USB flash drive*** - Router finds current firmware or configuration in the root directory of the connected USB device. • ***Both*** - looking for the current firmware or configuration from both sources.
Base URL	By parameter *Base URL* it is possible to enter base part of the domain or IP address, from which the configuration file will be downloaded.
Unit ID	Name of configuration. If the Unit ID is not filled, then as the file name used the MAC address of the router. (The delimiter is a colon is used instead of a dot.)
Update Hour	Automatic configuration update starts 5 minutes after turning on the router and then every 24 hours or it is possible to set the time of automatic configuration in parameter *Update Hour.* If the entered URL is different configuration than in the router then the router downloads this configuration and restarts itself.

Table 59: Automatic update configuration

The **configuration file** name is from parameter *Base URL*, hardware MAC address of ETH0 interface and *cfg* extension. Hardware MAC address and *cfg* extension is connected automatically and it isn't needed to enter this. By parameter *Unit ID* enabled it defines the concrete configuration name which will be download to the router. When using parameter *Unit ID*, hardware MAC address in configuration name will not be used.

The **firmware file** name is from parameter *Base URL,* type of router and bin extension.

The following examples find if there is a new firmware or configuration each day at 1:00 in the morning. An example is given on the type of router ER75i v2.

- Firmware: http://router.cz/er75i-v2.bin
- Configuration file: http://router.cz/temelin.cfg

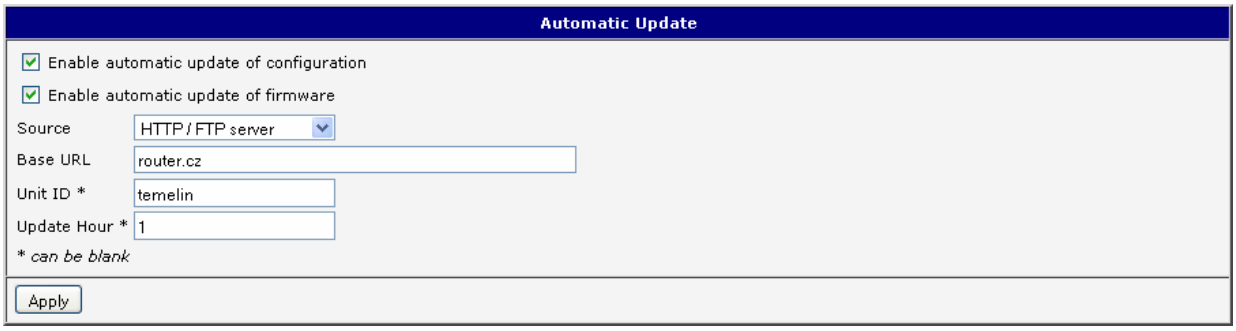


Fig. 60: Example of automatic update 1

The following examples find if there is a new firmware or configuration each day at 1:00 in the morning. An example is given on the type of router ER75i v2 with MAC address 00:11:22:33:44:55.

- Firmware: http://router.cz/er75i-v2.bin
- Configuration file: http://router.cz/00.11.22.33.44.55.cfg

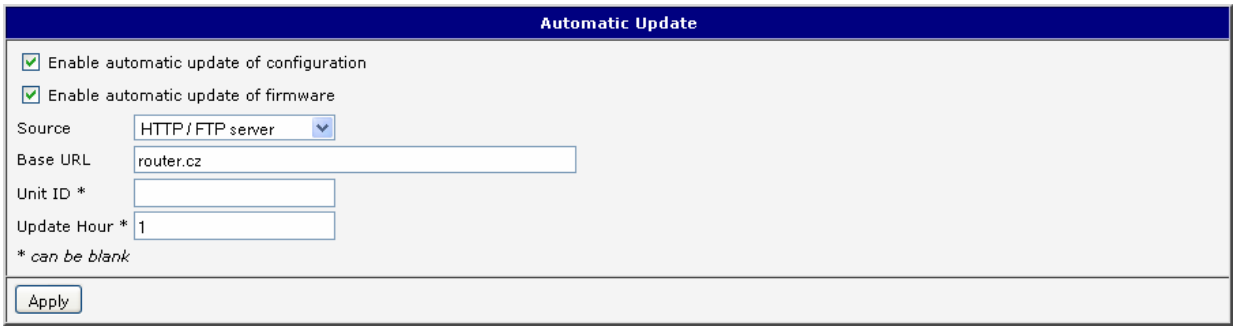


Fig. 61: Example of automatic update 2

1.28. *User modules*

Custom configuration of modules can be accessed by selecting the **Users Modules**. In the menu is possible add new software modules, remove them and move into their configuration. Programming, compiling and upload of user modules are described in the application programming guide.

Fig. 62: User modules

1.29. *Change profile*

To open the dialog box for changing profile select the **Change Profile** menu item. Profile switch is making by press the button *Apply*. Change take effect after restarting router by the help of button *Reboot* in web administration or by SMS message. It is possible select the standard profile or up to three alternative profiles. It is possible to copy actual configuration to selected configuration by selecting ***Copy settings from current profile to selected profile***.

Example of usage profiles: Profiles can be used for example to switch between different modes of operation of the router (router has compiled a PPP connection, the router has not compiled a PPP connection and the router creates a tunnel to the service center). Change the profile can then be done using a binary input, SMS or Web interface of the router.

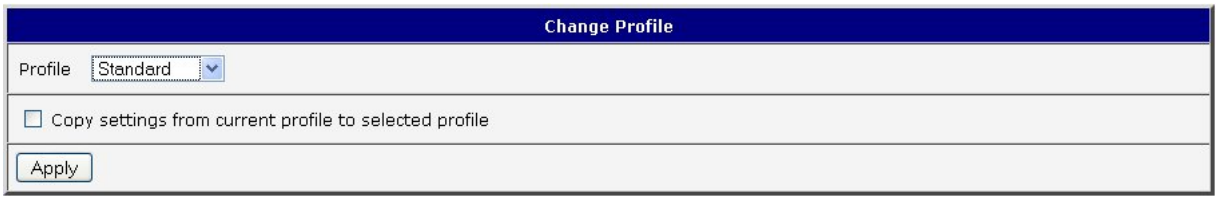


Fig. 63: Change profile

1.30. *Change password*

To open the dialog box for changing the access password select the **Change Password** menu item. The new password will be saved after pressing the *Apply* button.

In basic settings of the router the password is set on default form *root*. For higher security of your network we recommend changing this password.

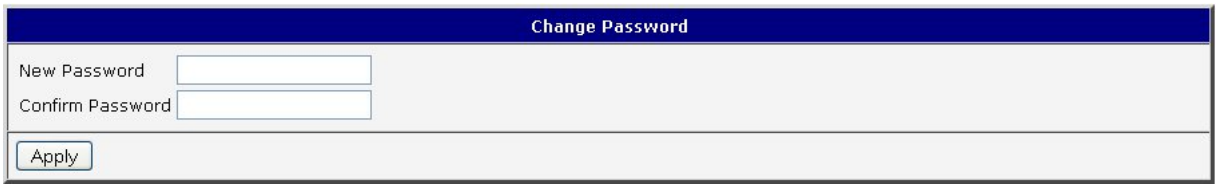


Fig. 64: Change password

1.31. *Set real time clock*

One - shot inner clock of the router setting can be called up in option **Set Real Time Clock** *item* in the menu. Clocks are set according to the engaged NTP server after push-button operation *Apply.*

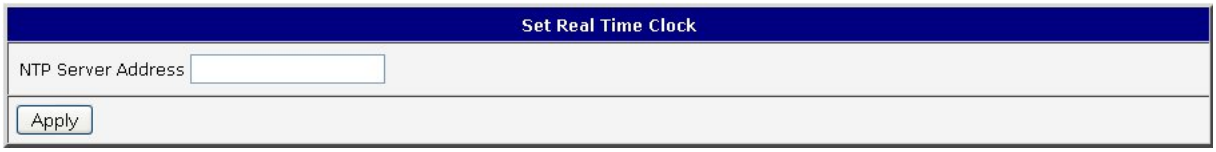


Fig. 65: Set real time clock

1.32. *Set SMS service center address*

The industrial router XR5i v2 is not availability item Set SMS service center address.

In some cases it is needed to set the phone number of the SMS service centre because of SMS sending. This parameter can not be set when the SIM card has set phone number of the SMS service centre. The phone number can be formed without international prefix xxx xxx xxx or with international prefix for example +420 xxx xxx xxx.

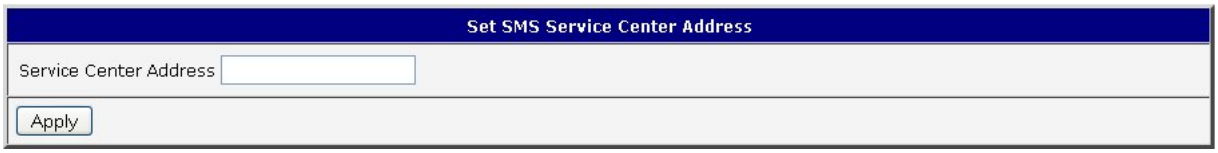


Fig. 66: Set SMS service center address

1.33. *Unlock SIM card*

The industrial router XR5i v2 is not availability item Unlock SIM card.

Possibility to unlock SIM PIN is under **Unlock SIM Card** item. If the inserted SIM card is secured by a PIN number, enter the PIN to field *SIM PIN* and push-button *Apply*.

SIM card is blocked after three failed attempts to enter the PIN code.

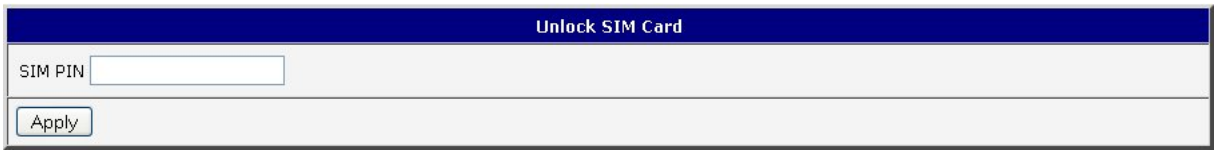


Fig. 67: Unlock SIM card

1.34. *Send SMS*

The industrial router XR5i v2 is not availability item Send SMS.

Sending SMS messages is possible in menu **Send SMS**. The SMS message will be sent after entering the **Phone number** and text SMS (**Message**) and by pushing button *Send.*

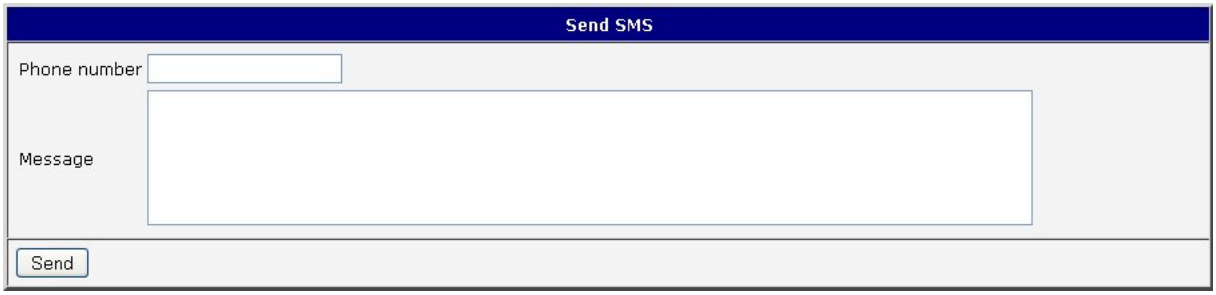


Fig. 68: Send SMS

SMS message sending via HTTP request is in the form:

*GET /send_exec.cgi?phone=%2B**420712345678**&message=**Test** HTTP/1.1*
Authorization: Basic cm9vdDpyb290

HTTP request will be sent to TCP connection on router port 80. Router sends an SMS message with text "*Test".* SMS is sent to phone number ""*420712345678"*. Authorization is in the format "user:password" coded by BASE64. In the example is used for root:root.

1.35. *Backup configuration*

The router configuration is possible to save by help of the *Backup Configuration* menu item. After clicking on this menu it is possible to check a destination directory, where it will save the router configuration.

1.36. *Restore configuration*

In case it is needed to restore the router configuration, it is possible in **Restore Configuration** menu item to check configuration by help **Browse** button.

Fig. 69: Restore configuration

1.37. *Update firmware*

To view the information about the firmware version and instructions for its update select the **Update Firmware** menu item. New firmware is selected via Browse button and update the following pressing the Update button.

Fig. 70: Update firmware

After successful firmware updating the following statement is listed:

Uploading firmware to RAM... ok
Programming FLASH..... ok

Reboot in progress

Continue here after reboot.

There is information about updating of the FLASH memory.

Upload firmware of different device can cause damage of the router!

During updating of the firmware permanent power supply has to be maintained.

1.38. *Reboot*

To reboot the router select the **Reboot** menu item and then press the *Reboot* button.

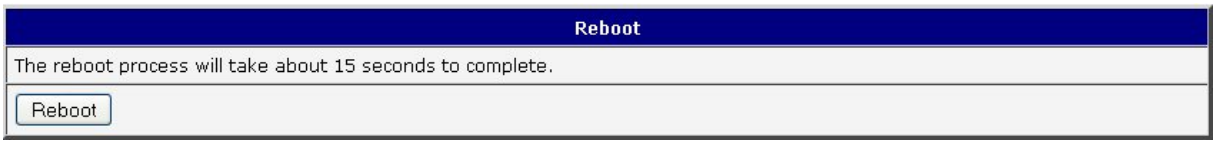


Fig. 71: Reboot

2. Configuration setting over Telnet

Attention! If the SIM card isn't inserted in the router, it is impossible for the router to operate. The Included SIM card must be activated for GPRS transmissions.

Monitoring of status, configuration and administration of the router can be performed by means of the Telnet interface. After IP address entry to the Telnet it is possible to configure the router by the help of commands. The default IP address of the modem is 192.168.1.1. Configuration may be performed only by the user "root" with initial password "root".

For Telnet exists the following commands:

Command	Description
cat	file contain write
cp	copy of file
date	show/change of system time
df	displaying of informations about file system
dmesg	displaying of kernel diagnostics messages
echo	string write
email	Email send
free	displaying of informations about memory
gsmat	AT commend send
gsminfo	displaying of informations about signal quality
gsmsms	SMS send
hwclock	displaying/change of time in RTC
ifconfig	displaying/change of interface configuration
io	reading/writing input/output pins
ip	displaying/change of route table
iptables	displaying/modification of NetFilter rules
kill	process kill
killall	processes kill
ln	link create
ls	dump of directory contain
mkdir	file create
mv	file move
ntpdate	synchronization of system time with NTP server
passwd	password change
ping	ICMP ping
ps	displaying of processes information
pwd	dump of actual directory
reboot	reboot
rm	file delete
rmdir	directory delete
route	displaying/change of route table
service	start/stop of service
sleep	pause on set seconds number
slog	displaying of system log
tail	displaying of file end
tcpdump	monitoring of network
touch	file create/actualization of file time stamp
vi	text editor

Table 60: Telnet commands